NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL REPORT

The Concurrent Implementation of Radio Frequency Identification and Unique Item Identification at Naval Surface Warfare Center, Crane, IN as a Model for a Navy Supply Chain Application

---

By: Ernan Obellos
Travis Colleran
Ryan Lookabill

December 2007

Advisors: Geraldo Ferrer
Nick Dew

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE				*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2007	**3. REPORT TYPE AND DATES COVERED** MBA Professional Report		
4. TITLE AND SUBTITLE: The Concurrent Implementation of Radio Frequency Identification and Unique Item Identification at Naval Surface Warfare Center, Crane, IN as a Model for a Navy Supply Chain Application				**5. FUNDING NUMBERS**
6. AUTHOR(S) Obellos, E. S., Colleran, T. P. & Lookabill, R. D.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000				**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A				**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this report are those of the author(s) and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited				**12b. DISTRIBUTION CODE**

13. ABSTRACT *(maximum 200 words)*

The purpose of this MBA project is to conduct an analysis of a concurrent implementation of Unique Item Identification (UID) and Radio Frequency Identification (RFID) at the Naval Surface Warfare Center at Crane, Indiana (NSWC Crane). This project will use the developments put into place at the Space and Naval Warfare Systems Command (SPAWAR) Extremely High Frequency (EHF) Satellite Communications (SATCOM) Branch in San Diego as a baseline for the implementation at NSWC Crane. This project will provide a concurrent RFID/UID implementation plan for NSWC Crane's primary warehouse facility and conduct a Knowledge Value-Added analysis of that implementation.

14. SUBJECT TERMS Radio Frequency Identification, RFID, Unique Item Identification, UID, Concurrent Implementation, Asset Visibility, Automated Information Technology, AIT			**15. NUMBER OF PAGES** 121
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE CONCURRENT IMPLEMENTATION OF RADIO FREQUENCY IDENTIFICATION AND UNIQUE ITEM IDENTIFICATION AT NAVAL SURFACE WARFARE CENTER, CRANE, IN AS A MODEL FOR A NAVY SUPPLY CHAIN APPLICATION

Ernan S. Obellos, Lieutenant Commander, United States Navy

Travis P. Colleran, Lieutenant Commander, United States Navy

Ryan D. Lookabill, Lieutenant Commander, United States Navy

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL

December 2007

Authors: ________________________________

Ernan S. Obellos

____

Travis P. Colleran

____

Ryan D. Lookabill

Approved by: ________________________________

Geraldo Ferrer, Lead Advisor

____

Nick Dew, Support Advisor

____

Robert N. Beck, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

THE CONCURRENT IMPLEMENTATION OF RADIO FREQUENCY IDENTIFICATION AND UNIQUE ITEM IDENTIFICATION AT NAVAL SURFACE WARFARE CENTER, CRANE, IN AS A MODEL FOR A NAVY SUPPLY CHAIN APPLICATION

ABSTRACT

The purpose of this MBA project is to conduct an analysis of a concurrent implementation of Unique Item Identification (UID) and Radio Frequency Identification (RFID) at the Naval Surface Warfare Center at Crane, Indiana (NSWC Crane). This project will use the developments put into place at the Space and Naval Warfare Systems Command (SPAWAR) Extremely High Frequency (EHF) Satellite Communications (SATCOM) Branch in San Diego as a baseline for the implementation at NSWC Crane. This project will provide a concurrent RFID/UID implementation plan for NSWC Crane's primary warehouse facility and conduct a Knowledge Value-Added analysis of that implementation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADUSD (SI):	Assistant Deputy Under Secretary of Defense for Supply Integration
AES:	Applied Enterprise Solutions
AIDC:	Automatic Identification Data Capture
AIS:	Automated Identification Systems
AIT:	Automated Identification Technology
AOR:	Area of Responsibility
BCA:	Business Case Analysis
BRE:	Bangor Radio Frequency Evaluation
C4ISR:	Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance
C&A :	Certification and Authorization
CA :	Certification Authority
CAC:	Common Access Card
CENTCOM:	Central Command
CFFC:	Commander Fleet Forces Command
CIO:	Chief Information Officer
COCOM:	Combatant Commander
COLTS:	Catalog Ordering Logistics Tracking System
COMFISCS	Commander Fleet and Industrial Supply Centers
CONUS:	Continental United States
DAA:	Designated Approving Authority
DITSCAP:	DoD Information Technology Security and Accreditation Process
DoD:	Department of Defense
DoN:	Department of the Navy
EAS:	Electronic Article Surveillance
EEDSKs:	Early Entry Deployment Support Kits
EHF:	Extremely High Frequency

EUCOM:	European Command
FCC:	Federal Communications Commission
FHA:	Federal Highway Administration
FISC:	Fleet and Industrial Supply Center
FY:	Fiscal Year
HF:	High Frequency
IA:	Information Assurance
IAM:	Information Assurance Manager
IAP:	Information Assurance Program
IBTTA:	International Bridge and Turnpike Association
IFF:	Identification Friend of Foe
INCONUS:	Inside the Continental Untied States
IPT:	Integrated Process Team
ITV:	In-Transit Visibility
KVA:	Knowledge Value Added
LF:	Low Frequency
MCPC:	Market Comparable Process Cost
MCR:	Market Comparable Revenue
MW:	Microwave
NAVCIRT:	Navy Certified Incident Response Team
NAVSUP:	Naval Supply Systems Command
NCIMS:	NSWC Crane Inventory Management System
NCIMS – DBA:	NCIMS – Data Base Administrator
NCIMS – A:	NCIMS – Administrator
NETWARCOM:	Naval Network Warfare Command
NOLSC:	Naval Operations Logistics Support Center
NRFI:	Not Ready for Issue
NSN:	National Stock Number
NSWC:	Naval Surface Warfare Center
OCONUS:	Outside the Continental Untied States

OPNAV:	Office of the Chief of Naval Operations
PACOM:	Pacific Command
POC:	Points of Contact
POM:	Program Objective Memorandum
PDKs:	Portable Deployment Kits
PHIMS:	Philadelphia Inventory Management System
RF:	Radio Frequency
RFI:	Ready for Issue
RFID:	Radio Frequency Identification
ROI:	Return on Investment
ROK:	Return on Knowledge
SATCOM:	Satellite Communications
SNT:	Serial Number Tracking
SOAP:	Service Oriented Architectural Protocol
SOPs:	Standard Operating Procedures
SOUTHCOM:	Southern Command
SPAWAR:	Space Warfare Systems Command
SSAA:	System Security Authorization Agreement
TAC-VAT:	Total Asset Configuration – Visibility and Tracking
TAV:	Total Asset Visibility
UHF:	Ultra High Frequency
UID:	Unique Item Identification
UPC:	Universal Product Code
USD (AT&L):	Under Secretary of Defense Acquisition Technology and Logistics
USN:	United States Navy
VIN:	Vehicle Identification Number

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The authors would like to thank all the individuals that have contributed to the successful completion of this project. Specifically we would like to thank Drs. Geraldo Ferrer, Nick Dew and Thomas Housel for their instruction and guidance throughout this process; Ms. Jane Zimmerman of COMFISCS for making us part of the team and for her vision that the ultimate beneficiary should always be the war fighter; Mr. Y. Y. Wong and Mr. Barry Jones who provided us with a crash course in all things RFID and UID and helped to form the basis for our project; Mr. Bill Henley whose technical knowledge proved invaluable; and Captain Fulton and Ms. Judy Melton of NSWC Crane who provided us the information and access that was essential to the entire project. To all those individuals both named an unnamed we would like to say thanks for all that you have done.

Ernan S. Obellos, Travis P. Colleran and Ryan D. Lookabill

LCDR Ernan Obellos would like to express his appreciation to his family, teammates, professors and friends for the encouragement and directions they have bestowed to make this project a success. Mostly, he would like to thank his wife Terry, his sons Kristopher and E.J., and his daughter Isabella for being with him in every duty stations he's ever been.

Ernan S. Obellos

LCDR Travis Colleran would like to thank his teammates for the extraordinary efforts that made this project a reality and his family and friends for the love and support that they provided throughout this entire process. He would especially like to thank his wife, Merrie, and his daughters, Shelby and Reese, without whom none of this accomplishment would have been possible.

Travis P. Colleran

LCDR Ryan Lookabill would like to express his gratitude to his teammates, family, and friends for the help and guidance they provided throughout this endeavor. Specifically, he would like to thank his wife, Julia, for always being there to provide the encouragement and support that made this project possible.

Ryan D. Lookabill

I. INTRODUCTION

A. BACKGROUND

Logisticians in the Department of the Navy (DoN), in direct support of combat forces, do not have a standardized and precise picture of materiel movement in the theater of operations. Each Carrier Strike Group (CSG) has several beach detachments responsible for managing their own logistics pipeline. Unfortunately, this system decreases the onboard manpower of deployed groups. At the same time, the accuracy of information managed by these detachments carries a high level of error because of manual data collection and reporting.

The same issues are present with the movement and inventory management of DoN materiel in the continental United States (CONUS). The absence of auto-identification systems (AIS) to enhance materiel availability and movement information causes ineffective inventory management, waste of scarce assets, and inefficiency in support of deployed and CONUS units. As cited by Honorable Alan F. Estevez, Assistant Deputy Under Secretary of Defense for Supply Chain Integration (ADUSD (SI)), these shortfalls "ultimately affected the war-fighters' overall materiel readiness, their ability to close the force, and the operational availability of weapon systems. Furthermore, he indicated that the lack of synthesized, end-to-end, real-time information on items at rest and in transit undercut the combatant commander's ability to exercise directive authority for logistics."[1] What Mr. Estevez has described is the lack of asset visibility.

"Visibility" is the key word used to refer to the availability of information on assets that are both in transit as well as stationary. However, in military logistics,

[1] Alan F. Estevez, (2006). Army Logistician Bulletin. Retrieved on September 26, 2007, from http://www.almc.army.mil/ALOG/issues/MayJun05/pdf/alog_may_jun_05.pdf.

visibility is not an end in itself. Visibility is a tool that helps to manage end-to-end capacities and available assets across the supply chain to best support war-fighter requirements.[2]

Radio frequency identification (RFID) and Unique Item Identification (UID) are enabling technologies that allow military logisticians to synthesize and integrate end-to-end information about assets. Using both of these automated identification technologies (AITs) in concert will improve asset visibility when interfaced with a local supply chain database system. Our project will introduce a new concept of concurrent implementation of both RFID and UID for a more improved end-to-end supply chain management strategy.

B. PURPOSE

The purpose of this project is to identify the typical Navy Supply material operational processes as seen at Naval Surface Warfare Center Crane, IN (NSWC Crane). We will then use that information as a basis for identifying the right AIT for those operational processes and provide an outline for a RFID/UID concurrent implementation plan that best applies to NSWC Crane. We will conclude with a Knowledge Value Added (KVA) Return on Investment (ROI) analysis of the RFID/UID implementation plan.

C. SCOPE

UID and RFID implementation has been mandated by the Department of Defense (DoD). Despite these mandates, not all Navy organizations have fully implemented and efficiently utilized these technologies. Certain organizations have acted quickly and effectively to implement AITs in order to improve their operations. Other organizations

[2] Alan F. Estevez, (2006). Army Logistician Bulletin. Retrieved on September 26, 2007, from http://www.almc.army.mil/ALOG/issues/MayJun05/pdf/alog_may_jun_05.pdf.

have either rushed to comply with the RFID/UID mandate without a carefully developed implementation plan or have made little to no effort to adopt these technologies. This project addresses the concurrent implementation of RFID/UID technologies at the organizational level by producing an effective implementation plan and a KVA ROI analysis for this implementation at NSWC Crane.

D. METHODOLOGY

The methodology applied in this research project consists of the following steps:

1. Conduct a literature review of books, magazine articles, electronic media, and other library resources.

2. Conduct a thorough review of RFID technology.

3. Conduct a thorough review of UID technology.

4. Conduct a review of the current RFID and UID mandates and implementations in DoD.

5. Conduct a site visit to Space and Naval Warfare Systems Command (SPAWAR) San Diego, CA.

6. Observe and analyze current RFID/UID applications at SPAWAR San Diego.

7. Conduct a site visit to NSWC Crane.

8. Conduct a review and analysis of typical Navy materiel logistics processes as observed at NSWC Crane.

9. Build an effective RFID/UID implementation plan that will translate to typical Navy materiel logistics processes.

10. Conduct a KVA ROI analysis of the RFID/UID implementation at NSWC Crane.

11. Prepare a summary and make recommendations.

THIS PAGE INTENTIONALLY LEFT BLANK

II. RFID

A. RFID TECHNOLOGY[3]

RFID can easily be explained as an AIT that uses radio wave technology. Since radio waves are known to reach any distance on this planet, auto-identification of any object or person is possible using RFID. A basic example is identification of a military member by reading his or her DoD identification card. RFID has the capability to store the entire military member's information and to have that information retrieved remotely using radio waves as a medium of carrying the data.

According to Sandip Lahiri, RFID is just one of the AITs, other commonly used systems are: bar code, biometric, voice identification, and optical character recognition. Auto-ID is a part of a system, whether with accounting or inventory application, to identify anything without human intervention. In most cases, this system is coupled with Automatic Identification Data Capture (AIDC); information is entered into a computer database without a person typing it in. The goals of Auto-ID systems are to optimize efficiency, reduce errors from human data entry, and dedicate personnel efforts to other important task such as customer service.[4]

1. Bandwidth

The bandwidth of the radio wave, also known as radio frequency (RF), determines specific RFID applications as prescribed or allocated by local authorities. Authorized RF ranges are the following: 125-134 kHz (LF: low frequency), 13.56 MHz (HF: high frequency), 315-433 MHz or 868-915 MHz (UHF: ultra-high frequency), 2.45 GHz or

[3] Parts of this section are drawn from Sandip Lahiri, (2005). *RFID Sourcebook*. Upper Saddle River, NJ: IBM Press. pp. 1-48.

[4] What is automatic identification? RFID Journal. Retrieved on July 14, 2007, from http://www.rfidjournal.com/faq/16/49.

5.8 GHz (MW: microwave). Provided in Table-1 are details of RF ranges with respective read distances, read rates, antenna size, and types of operating environments.

Table 1. RFID RF ranges and characteristics.[5]

Band	Frequency Range	Operating Environment	Antenna size	Read rate	Read distance
LF	**125-134kHz**	**Metals, liquids, dirt, snow, mud**	**Largest**	**Lowest**	**Less than 1 foot**
HF	**13.56MHz**	**Fair on metals & liquids**	**Large**	**Low**	**About 3 feet**
UHF	**315-433Mhz**	**Poor on metals & liquids**	**Small**	**High**	**About 30 to 300 feet**
MW	**2.45 or 5.8GHz**	**Very poor on metals & liquids**	**Smallest**	**Very high**	**About 100 feet**

[5] U. M. Apte, N. Dew, & G. Ferrer, (2006). What is the Right RFID for Your Process? *Acquisition Research Sponsored Report Series,* 3, 9.

2. RFID System

The most basic RFID system is made of three major components: a tag or tags made of different materials for specific applications, a reader which is also known as an interrogator to communicate with the tags, and the system supporting infrastructure composed of both hardware and software. In some applications, the software is also frequently identified as the middleware.[6]

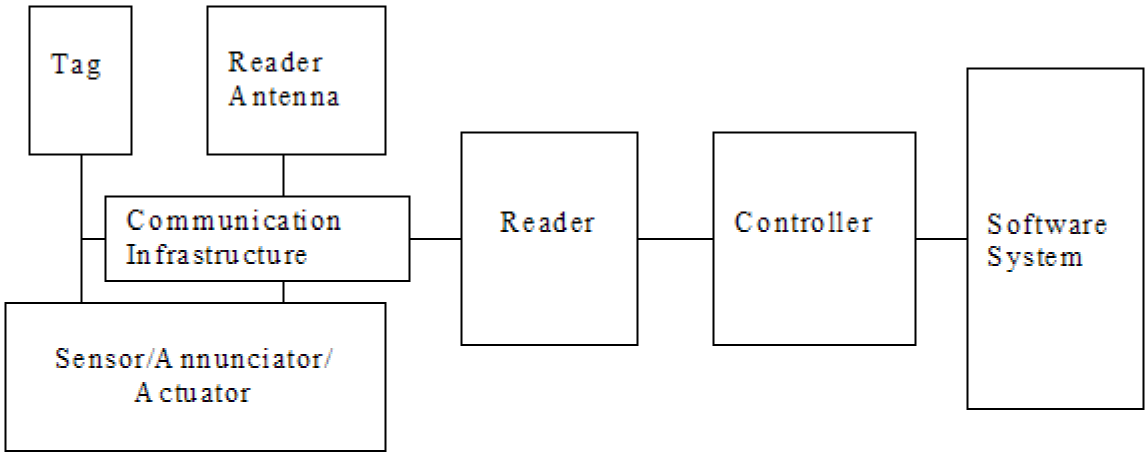
From an end-to-end perspective, the system is composed of the following components:

- Tag – A mandatory component, and is a device attached to the material or person to be identified.
- Reader – A mandatory component and functions to transmit and receive signals from the tag.
- Reader antenna – A mandatory component attached to the reader. Most of the newer readers have built-in antennas.
- Controller – A mandatory component of the reader. Some newer reader models have built-in controllers.
- Sensor, actuator, and annunciator. – Are optional components required to record system external input and output.
- Host and software system – Functions as a processor of captured Auto ID information to become an RFID solution.
- Communication infrastructure – A mandatory component composed of both wired and wireless circuitries needed to connect all above components. This enables the system to communicate with each other.

A schematic diagram of this system is illustrated in Figure-1.

[6] Office of the Privacy Commissioner of Canada. Fact Sheet: RFID Technology. Retrieved on June 12, 2007, from http://www.privcom.gc.ca/fs-fi/02_05_d_28_e.asp.

Figure 1. RFID System Components Schematic Diagram.



a. Tag

RFID tags are also known as transponders. In most cases, these are small pieces of material such as regular hanging identification tags. Each tag has three major parts: an antenna, a microchip unit, and a casing to protect both antenna and the microchip. The antenna receives the signal transmitted by the reader and can be three-dimensional for improved signal absorption rate. The microchip unit contains memory storage which varies in capacity depending on the type of tag. The microchip units can also have either read-only or read-write capabilities.

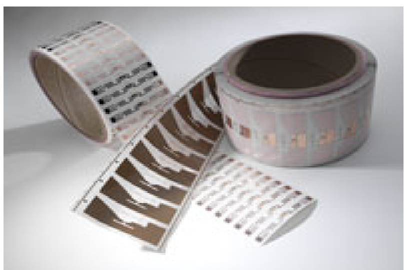
A read-only microchip is used in RFID tags with purposes of initial identification and with the intent that the tag will carry the same information during the tag's life expectancy. For example, tags attached to automobiles when manufactured contain information such as vehicle identification number (VIN), chassis serial number, engine serial number and date manufactured; information that will not change during the course of the vehicle's life.[7] Read-only tags can also be used to identify pallet shipments and then can be discarded after use.

[7] RFID use growing in automotive manufacturing process. (2007). *Industry Week*. Retrieved on July 13, 2007, from http://www.industryweek.com/ReadArticle.aspx?ArticleID=11774.

Chips with read-write capabilities are used in tags with a "recycle feature". Information stored on the tag can be modified or erased as needed. The ability to "recycle" these tags demands a premium in cost compared to the read-only tags.[8]

Among the read-only and rewritable RFID micro-chips there are three types of tags: passive, active and semi-passive. Figure 2 depicts a few examples of all three types used in industry today.

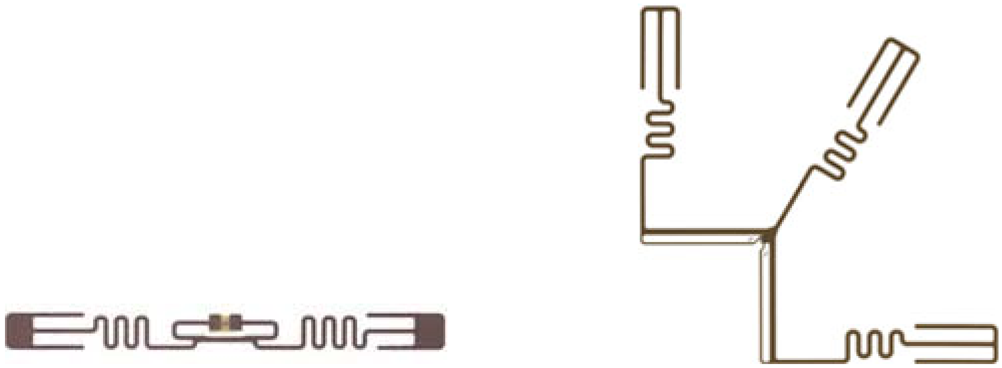
Figure 2. Examples of RFID tags.



1. Passive RFID tag. A Passive RFID tag has no power of its own; rather, it energizes itself by using the power from the reader and then sends back the stored data. The tags are energized by the RF induced in the antenna (Figure 3) which was transmitted from the reader. This powers the micro-chip circuitry which sends the coded signal back to the reader when the tag is interrogated. Advantages of the passive tag are longer life, lower unit cost and smaller size.

[8] RFID use growing in automotive manufacturing process. (2007). *Industry Week*. Retrieved on July 13, 2007, from http://www.industryweek.com/ReadArticle.aspx?ArticleID=11774.

Figure 3. Examples of antennas used in passive tags.



A passive tag can have a life expectancy of twenty years or more because it is not dependent on a battery for power. Passive tags are also the cheapest and smallest among all types allowing for a wider range of applicability. Disadvantages of passive tags are shorter "read" distance capability between the reader and the tag, limited ability of using electrical power due to sensor constraints, and the extended life expectancy can actually induce erroneous information to the database when the item the passive tag was identified with is moved, sold, or discarded.

2. Active RFID tag. Active RFID tags have an inherent power supply which is typically sourced from a battery. Some active tags can have a ten-year life expectancy. The power source energizes the microchip's circuitry and the tag has a transmitter that continuously sends out a signal to a reader. Major advantages of active tags are longer "reading" distance and the capability to record external temperatures by using internal electronics such as microprocessors and sensors. Known major disadvantages are battery operation dependence which limits lifetime expectancy, active tags are more expensive and they are much larger in size which may limit applicability. Long term maintenance cost may also be uneconomical if the battery has to be replaced.[9]

3. Semi-passive RFID tag. Semi-passive tags have transmitters and receivers also known as transponders. They have their own power supply from a

[9] U. M. Apte, N. Dew, & G. Ferrer, (2006). What is the Right RFID for Your Process? *Acquisition Research Sponsored Report Series,* 3, 15.

battery and become active only when receiving the "correct" coded signal from the reader interrogator, thus using the battery power only when transmitting the signal back. In the absence of the coded signal, the tag ceases signal transmission prolonging the life expectancy of the battery and the tag as well. Advantages are extended read distance rates over the passive tag, longer service life expectancy, and the ability to operate with sensors to record data such as temperatures. One disadvantage is the higher cost compared to the passive tag.[10]

When it comes to read ranges, the advantages of active and semi-passive tags are useful for tracking high-value goods by providing extended scanning ranges of one hundred feet or more between the reader and the tag. Applications such as locating either railway cars on a track in a major station hub, forty-foot container vans in shipping ports, or automobiles in manufacturing lots can benefit from both active and semi-passive tags. Passive tags, which cost just a few cents each if bought in volume, have applicability to both low and high cost items in shorter read ranges of less than twenty feet.[11] Table 2 lists the advantages, limitations and capabilities of the different types of RF tags.

Table 2. Tag types with RF types, advantages, limitations, and capabilities.

Tag type	Frequency type	Advantages	Limitation	Capabilities
Passive	All frequencies, mainly LF & HF	Best in cost, and life-span.	Identification only, less read range	Anti-theft, supply chain management, inventory control, access control, animal tagging
Semi-Passive	All frequencies, mainly LF & HF	Better in cost, life-span, less sensors	Limited memory, battery dependent	Pallet-level of supply chain management, inventory control, environmental control
Active	All frequencies, mainly UHF & MW	High memory, reading range, more sensors	High cost, battery dependent	Inventory management and control, electronic toll collection, real time location management

10 Sensing New RFID Opportunities. *RFID Journal*. Retrieved on July 13, 2007, from http://www.rfidjournal.com/article/articleview/2081/1/2/.

11 The Basics of RFID Technology. *RFID Journal* Retrieved on June 12, 2007, from http://www.rfidjournal.com/article/articleview/1337/1/129/.

b. Reader

An RFID reader, which is also called an interrogator, is a part of the system that transmits and receives information from the RFID tag. One function of the reader is to provide energy to a passive type tag. The radio frequency emitted by the reader is converted into an electrical field which a passive tag will use to energize itself when transmitting the information back. Depending on purpose and operation, a reader can be handheld or a fixed model.

A handheld is used mainly for inventory purposes where the unit can be carried around to scan stationary, tagged materials. An example is scanning tagged items on bins or bulky materials in warehouses. A stationary or fixed device is used to read tags that are mobile within the area of operation. In most transshipment operations, these readers are installed in receiving or shipping bay doors. For "read efficiency," they can be installed on both sides of the bay doors as well as overhead of the cargo flow.[12] In operations such as a repair depot, the same stationary set-up can be used to track repair movement of materials.

c. Reader Antenna

A reader antenna enables communication between the reader and the tag. The reader antenna and the reader are two different devices connected to each other by a cable with a length of between six to twenty-five feet. In most models, a reader has the capability of supporting a maximum of four reader antennas.

The function of a reader antenna is to send the reader transmitter RF signal within the operating environment and at the same time receive the signal back from the tag for the reader. It is imperative that antennas are positioned properly to maximize reading accuracy. In most cases, antennas are shaped like square boxes or rectangular as pictured in Figure 4.

---

[12] The Basics of RFID Technology. *RFID Journal.* Retrieved on June 12, 2007, from http://www.rfidjournal.com/article/articleview/1337/1/129/.

Figure 4. Models of Reader Antennas.

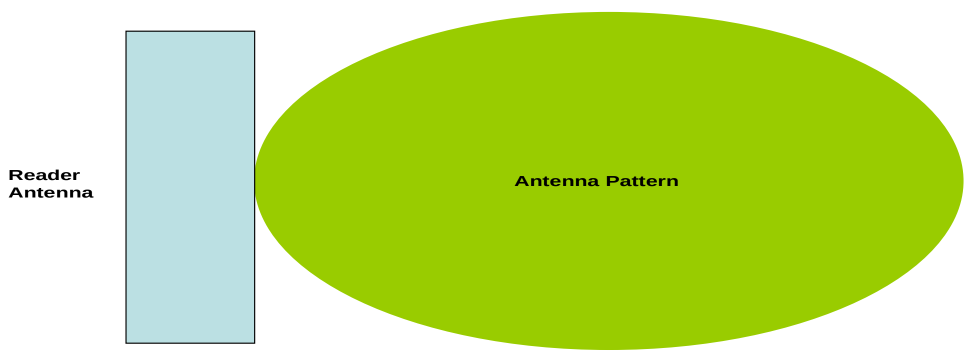
Alien Technology

Intermec Model

Omron

Reader antennas have a footprint which dictates the read area. This is also known as the read zone, read window or antenna pattern. This footprint is ellipsoid or balloon shape, projecting outward from the front of the antenna, and is three-dimensional in nature. Within this footprint, read accuracy and rates are optimized. Below is an illustration of an antenna footprint.

Figure 5. Antenna Footprint



Simple antenna footprint/pattern

d. Controller

A controller can best be described as a medium that the host computer, or any other external entity, uses to communicate with the reader. An easier analogy to aid in understanding is to compare this to a printer driver of a printer device. For a computer to print the processed data, the computer must have the printer driver in its system. In a similar way, the controller allows the host computer to retrieve data from the reader. A controller can be a component by itself, or built into the reader. Most new production models have the controllers embedded inside the reader devices.

e. Sensor, Annunciator, and Actuator

A sensor provides the option for the reader to be either energized or to operate in a standby mode. A sensor functions as an automatic switch using external input such an object in motion that allows the reader to optimize efficiency.

An annunciator is an electronic signal or indicator used to provide status during tag reading operations. The annunciator is used in conjunction with alarms, colored and/or strobe lights that can provide audible and visual information when a tag is within the reading spectrum. The annunciator can energize alarms, strobes and/or red lights for tag reading errors, green lights for satisfactory data and yellow lights to signal a connection breakdown.

Actuators are mechanical devices used in conjunction with annunciators and sensors within the tag reading process of the RFID system. An example is a robotic mechanical access gate that will secure the flow of materials when the annunciator sends a signal indicating faulty tag data.

f. Host and Software System

The host and software system are the hardware and software components of the RFID system. They are external to the RFID hardware; the reader, tag, and

antenna. The host and software system is made up of four components: the edge interface system, the middleware, the enterprise back-end interface, and the enterprise back end.

1. The edge interface system. The edge interface component integrates the host and software system with the RFID hardware. The edge interface's functions are to ascertain data from the readers, command the reader's function, and utilize the readers to trigger the externally connected actuators and annunciators. Furthermore, this component is a super-controller that can screen and reconcile duplicate readings from adjacent or different readers and allow automatic activation of annunciators or actuators when programmed for specific events. It also selectively filters tag data being sent to the host and software system and allows for the remote management of all attached readers.

2. The middleware. The middleware component can best be described as controlling all the functionalities between the edge interface and the back-end interface of the enterprise. As the central nervous system of the RFID system, the middleware facilitates data sharing within or external of the enterprise, optimizes efficiency management of data produced by the RFID system, enables implementation of business specific applications, and provides compatibility with other software systems.

3. The enterprise back-end interface. The enterprise back-end interface component combines the functions between the middleware and the enterprise back-end components. This component allows for specific business applications to be integrated. Integration of specific business processes determines the complexity of this component and the more complex the business process indicates the amount of effort required to build the interface. In most cases, a generic interface is needed to initiate data transfer transactions between the interface and the enterprise back-end components.

4. The enterprise back-end. The enterprise back-end component includes all of the applications and hardware systems of an enterprise. This includes all

the program applications required to run the business processes and the complementing data storage for the whole enterprise. From the perspective of integrating an RFID system with the enterprise back-end the compatibility adjustment is minimal on the back-end side. The back-end usually had been pre-existing and functional and therefore can be easily integrated with the edge interface, middleware, enterprise back-end interface, and the new RFID system.

g. Communication Infrastructure

The communication infrastructure furnishes connection between all components of the RFID and enterprise systems. It also supports system security and system management as an integral component of the RFID system. Connection between components can be wired or wireless, depending on the layout of the system. Wireless capabilities may include Bluetooth wireless products in a personal area network (PAN), a local area network (LAN), or a wide area network (WAN).

3. Other RFID Concepts, Technology Advantages and Limitations

a. Tag Collision

Tag collision is a situation in the RFID system process where more than one tag is trying to communicate back in response to the same reader. A reader may become confused when it receives simultaneous signals. In that case, the reader follows a "singulation protocol" and uses an anti-collision algorithm to resolve the tag collision issue.[13]

[13] The most commonly used anti-collision algorithms are ALOHA for HF and Tree Walking for UHF.

b. Reader Collision

Reader Collision is a condition when two read zones or read patterns of two or more readers overlap each other. This results when the antennas of two readers are positioned close to each other and overlap each other's read patterns; a destructive interference occurs. As a result, each antenna's RF signal is canceled out by the other. To preclude this, an antenna has to be installed in such a way that it does not face another antenna from a different reader.

c. Tag Readability

Tag readability is the capability of an RFID system to successfully read tags in a specific environment. To maximize readability, the design of the system has to transmit multiple queries from the reader to the tags. This improves the read probabilities in case the first or second queries were unsuccessful. The number of queries is induced by the reader controller and directed by the middleware. The desired end-state is to have only one successful read, therefore the system also has a filter capability that precludes multiple readings of the same tag.

d. RFID Technology Advantages

1. Contact-less. No contact between the readers and tags precludes wear and tear and improves operation efficiency. An automatic and simultaneous reading of several tags within the read area without contact also enhances the processing time required.

2. Writable data. This enables tags to be recycled from 10,000 to 100,000 times if needed. This feature will prove to be economical for some applications where information can be added or deleted or even erased on the same tag. An example

of an application which will benefit from writable data includes a tag that requires time stamping or recording of external temperatures to which it was exposed.

3. Line of sight independent. The ability of an RFID system to read and write data through obstructing objects is one of the most process-enhancing capabilities of the system. For example, the cargo of a truck driving through the cargo bay can all be automatically read without line of sight requirements for each tag. Prior to RFID, this operation would have involved the time-consuming process of off-loading the truck.

4. Multi-read ranges. Depending on the RF required, the choice of tags to optimize read range and cost is an available option. An operational environment which does not require extensive read distance capabilities can use a cheaper, passive, low-frequency tag. As demonstrated in an environment with a wide-spread inventory, like a car manufacturer storage lot with thousands of vehicles, the benefit from the extended read-range of a UHF active tag to identify and locate a specific unit is quickly realized.

5. Variety data-capacity range. Depending on manufacture and intended use, a tag can carry a variety of bit or memory capacity to fit the application requirement. Currently, RFID tag market availability varies from 1 to 96 bits and even more in some special applications. This variability allows the users to optimize operations cost by utilizing the type of tag required and minimize the cost based on the level of memory capacity needed.

6. Multiple tag read options. Using the previously mentioned anti-collision tag algorithm, the reader can auto-identify multiple tags both in motion or

stationary. This capability allows the reader to process the data simultaneously instead of reading one tag at a time. This feature also minimizes, if not precludes, tag read errors and vastly improves read time.

7. Durable. With countable moving parts, tags can operate and sustain harsh environmental conditions such as high humidity, heat, vibration, water and shock. The temperature survivability for some passive tags can range from -40 to 400 degrees Fahrenheit.

8. Smart task enhancer. Performance of tasking, such as recording temperature exposure in the case of the food industry, enhances the overall operation efficiency. Anti-theft application uses long range active RFID tags for luxury vehicles or any high- value item. As previously mentioned, the use of the sensors and actuators presents numerous options to enhance efficiency in a particular operational environment.

B. HISTORY OF RFID[14]

This section concerns the history of RFID from its pre-World War II beginnings, through the decades of research and development to present day applications. Table 3 at the end of this section shows major RFID milestones.

1. The 1930s and 1940s: Origins

RFID technology dates back to the 1930s and 1940s prior to and during World War II. The British, Germans, Japanese and Americans all used radar technology during the conflict. Radar, discovered in 1935 by a Scottish physicist, Sir Robert Alexander

[14] Parts of this section are drawn from The History of RFID Technology. *RFID Journal.* Retrieved on June 12, 2007, from http://www.rfidjournal.com/article/articleview/1338/1/129/ and from J. Landit,. (2001). Shrouds of time: *The History of RFID*, Retrieved on June 11th, 2007, from http://www.transcore.com/pdf/ AIM%20shrouds_of_time.pdf.

Watson-Watt introduced this new technology that was used by both the Allies and the Axis powers to detect and warn of approaching enemy planes before they were within striking distance. A problem arose, however, as there was no way to identify and determine if a plane was the enemy or if it was a friendly plane returning from a mission.

German scientists first discovered that Luftwaffe pilots could roll their plane's wings when returning to German territory and this would change the radar signal reflected back to the receiver. This rudimentary method alerted the German forces on the ground that the incoming planes were German and not the enemy. Essentially, this was the first application of a passive RFID system.

The British Government took that application a step further and designed the first identification friend or foe (IFF) system. Sir Watson-Watt headed a secret project to give the British a distinct advantage in the air war and placed a transmitter on each British plane. When a returning aircraft received a radio signal from a radar station on the ground, the plane broadcast a signal back to the radar station that identified the plane as friendly.

RFID operates on this same fundamental concept. A radio signal is sent to an RFID transponder, which when alerted, either reflects a signal in return (passive system) or sends a signal (active system).

2. The 1950s: Invention to Innovation

Significant advances in RF communications and radar systems continued in the 1950s. These advances spurred an era of exploration of RFID techniques. Numerous technologies related to RFID were investigated to include such efforts as F. L. Vernon's, "Applications of the microwave homodyne", and "Radio transmission systems with modulatable passive responder", by D.B. Harris. These developments were precursors to many new RFID applications in the 1960s and 1970s.

3. The 1960s: Beginnings of Realistic Application

In the 1960s, R.F. Harrington developed the electromagnetic theory related to RFID in his works “Field measurements using active scatterers” and “Theory of loaded scatterers”. At the same time, commercial applications were also gaining.

Two corporations, Sensormatic and Checkpoint, were started in the late 1960s. These corporations and others designed electronic article surveillance (EAS) equipment to deter theft in the marketplace. These types of systems applied the use of a 1-bit tag which allowed only the absence or presence of the tag to be detected. These tags were inexpensive to make and provided very effective anti-theft protection on merchandise. It can be argued that EAS was the first and most widespread commercial application of RFID.

4. The 1970s: Proliferation of Applications

During the 1970s inventors, developers, corporations, academic institutions, and government laboratories actively pursued RFID technology. Mario W. Cardullo claims to have earned the first U.S. patent for active RFID tags with rewritable memory on January 23, 1973. Also in 1973, Charles Walton, an entrepreneur from California, received a patent for a passive transponder used to unlock a door without a key. A card embedded with a transponder communicated a signal to the reader near the door. Once the reader detected the valid identity number stored within the RFID tag, the reader unlocked the door. Walton licensed the technology to the lock maker Schlage and several other corporations.

Other notable advances were being developed in research laboratories and academic institutions such as Los Alamos Scientific Laboratory, Northwestern University, and the Microwave Institute Foundation in Sweden. A crucial, early project was the Los Alamos development of “Short-range, radio-telemetry for electronic identification using modulated backscatter” in 1975. This work was eventually used to develop a system for tracking of nuclear materials by putting a transponder on a truck and

readers at the gates of secure facilities. The gate antenna would wake up the truck's transponder which would respond with an ID and potentially other information such as the driver's name.

Major American companies were also working to develop RFID technology. Raytheon invented the "Raytag" in 1973. RCA and Fairchild were active in their efforts, developing an "Electronic Identification System" in 1975 and an electronic license plate for motor vehicles in 1977. Thomas Meyers and Ashley Fairchild also designed a "Passive encoding microwave transponder" in 1978.

After a request from the U.S. Department of Agriculture, Los Alamos also developed a passive RFID tag to track cattle. Driving the need for RFID was the ability to track cows that were being given medicines and hormones when they were ill. It was very difficult to ensure that each cow received the correct dosage and wasn't given more than one dose accidentally. The scientists at Los Alamos developed a passive RFID system that used UHF radio waves with the tag drawing energy from the reader and reflecting a modulated signal back to reader. In later years, corporations developed a new system that utilized an LF radio wave that featured a smaller transponder. The glass encapsulated transponder could be injected under the cow's skin. Today, ranchers still use the system and variations of the original transponders are placed in key-cards and utilized to control access to buildings.

The Port Authority of New York and New Jersey were also trying out new systems built by General Electric, Westinghouse, Glenayre, and Philips. These systems produced some favorable results, but the first commercially successful transportation application of RFID, electronic toll collection, would not be ready for use on a large scale until the next decade. Also, The International Bridge and Turnpike Association (IBTTA), and the United States Federal Highway Administration (FHA) sponsored a conference in 1973 that concluded there was no national interest in developing a standard for electronic vehicle identification. This was a critical decision as it allowed a variety of systems to develop and gave the infant RFID technology a chance to grow and expand.

5. The 1980s: Implementation around the Globe

During the 1980s, new companies began to enter the RFID market. The number of companies working on RFID technology began to multiply and grow rapidly as RFID's potential had become obvious. One new corporation, Identronix, was an off-shoot of the Los Alamos Scientific Laboratory and other members from the Los Alamos team founded the company Amtech.

The mid-1980s started the era of global implementation of RFID technology, though various regions of the world were interested in different applications. The largest interests in the United States were for personnel access, animals, and transportation. The greatest interests in Europe were for short-range systems for animals, industrial and business applications. Additionally, toll roads in Italy, Spain, France, Portugal and Norway began to apply RFID technology.

Testing of RFID for toll collection had been going on for many years, but the first commercial application began in Norway in 1987. The United States followed quickly as the Dallas North Turnpike began using RFID technology in 1989. Also, during this period, the Port Authority of New York and New Jersey initiated commercial operation of RFID for buses accessing the Lincoln Tunnel that used both low and high frequency systems that offered greater range and faster data transfer rates.

6. The 1990s: RFID Technology Everywhere

The 1990's were a significant decade for RFID as it saw the wide-scale employment of electronic toll collection in the United States. Some of the most important applications included numerous developments in electronic tolling. The world's first open highway electronic tolling system began operation in Oklahoma in 1991. Vehicle owners who purchased a RFID Pass-tag could pass toll collection points at highway speeds, without stopping at toll plazas to pay. Video cameras were installed to enforce cars without the RFID pass-tags to stop and pay the toll.

The world's first combined toll collection and traffic management system began operation in the Houston, Texas in 1992 and another first was installed on the Kansas turnpike using an innovation based on the Title 21 standard with readers that could also operate with the tags used on the Oklahoma Toll System. Georgia’s State Highway 400 followed these firsts by upgrading their equipment with readers that could communicate with the new Title 21 tags as well as the legacy tags.

In 1990 in the Northeastern United States, several regional toll agencies formed a group, the E-Z Pass Interagency Group (IAG). The E-Z Group worked to develop a regionally compatible electronic toll collection system. This system became the model for using a single tag and single billing account per vehicle to access highways of several toll authorities.

With the success of electronic toll collection, many other new innovations followed to include the first multiple uses of RFID tags across various business segments. A single tag utilizing single or dual billing accounts could be applied in electronic toll collection, parking lot access, fare collection, and gated community and school access. In the Dallas-Fort Worth metro area, a major first was achieved when a single RFID tag on a vehicle could be utilized to pay tolls on the North Dallas Toll way, for parking access and payment, as well as access to gated communities and business properties. Also in the 90s, The Texas Instruments (TI) Company began developing the TIRIS system, a state of the art system, used in many automobiles for control of the starting of the vehicle engine. Other new applications were also developed for dispensing fuel, gaming chips, ski passes and vehicle access to name a few.

Research and development continued to boom in the 1990s as new technologies expanded the functionality of RFID. Another first was achieved when Schottky diodes were fabricated on a regular integrated circuit. This development allowed construction of microwave RFID tags that contained a single, integrated circuit that lead to tags that were smaller than existing tags and helped the proliferation of RFID into the 21st century.

7. The 21st Century and Beyond

The 21st century has also seen much new advancement in RFID technology. RFID utilization has been documented in mainstream media and will continue to be employed in everyday life with growing interest in telematics and mobile commerce. These new areas of use will bring RFID even closer to the consumer. As of late, the Federal Communications Commission (FCC) has allocated more bandwidth for major expansion of intelligent transportation systems with numerous new applications and service regarding RFID. In order to accommodate these new applications, more advanced RFID equipment must be developed and implemented.

Table 3. The Decades of RFID[15]

Decade	Event
1940 - 1950	Radar refined and used, major World War II development effort. RFID invented in 1948.
1950 - 1960	Early explorations of RFID technology, laboratory experiments.
1960 - 1970	Development of the theory of RFID. Start of applications field trials.
1970 - 1980	Explosion of RFID development. Tests of RFID accelerate. Very early adopter implementations of RFID.
1980 - 1990	Commercial applications of RFID enter mainstream.
1990 - 2000	Emergence of standards. RFID widely deployed. RFID becomes a part of everyday life.

[15] Table 3 is from J. Landit, (2001). Shrouds of time: *The History of RFID*, Retrieved on June 11th, 2007, from http://www.transcore.com/pdf/AIM%20shrouds_of_time.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

III. UID

A. UID TECHNOLOGY[16]

1. Beginning with the Bar Code

Unique Item Identification (UID)[17] takes its roots from the bar code. A bar code is a series of black stripes printed on a white background. The unique arrangement of the stripes can be scanned, read and interpreted by a computer using a bar code system. The reading process only requires a micro-second and is comparatively error free. The process of reading a bar code uses reflectance and absorption of light which is similar to reading text on a white paper. Movement of a specific light wavelength to a bar code at a consistent speed produces a reflection which is measured by a photoreceptor. The intermittent white and black pattern of the bar codes produces an electrical wave. This electrical wave is sent to the "chip decoder" which deciphers the signal using an established bar code system, also known as bar code symbology. [18]

2. From One-Dimension to Two

A one-dimensional or "1D" bar code system only measures the width of the black bars and the related white spaces in between. A 1D bar code only contains a little more than 12 characters. The codes identified with this limited number of characters typically have expanded information built within a corresponding database. For example, a vehicle license plate, which is composed of a few alpha-numeric combinations of

[16] Parts of this section are drawn from Two Dimensional Bar Code Overview. (2006). Retrieved on September 26, 2007, from http://www.dataintro.com/lit/wp2dbarcodes.pdf.

[17] For the purposes of this project UID is synonymous with Item Unique Identification (IUID).

[18] Bar code symbology is the language used by bar code systems. Each symbology represents a specific character by using a unique width, length and color intensity of the white and black spaces, designed for a specific application. The most commonly used bar code symbologies are UPC, Code 39, PDF 417, Codabar and DataMatrix.

characters, can be matched to additional information such as the registered owner, the VIN number, make and model of the vehicle, etc.

In contrast, the two-dimensional bar code, or "2D" uses the width and height of the black bars and the white spaces in between them. As an advantage, the amount of data that each character represents is significantly greater than 1D. In most 2D symbology, a bar code the size of a mail stamp can store over a thousand alpha-numeric characters. The advantage compared to 1D is that this data will ride with the item being identified instead of requiring retrieval from a database.

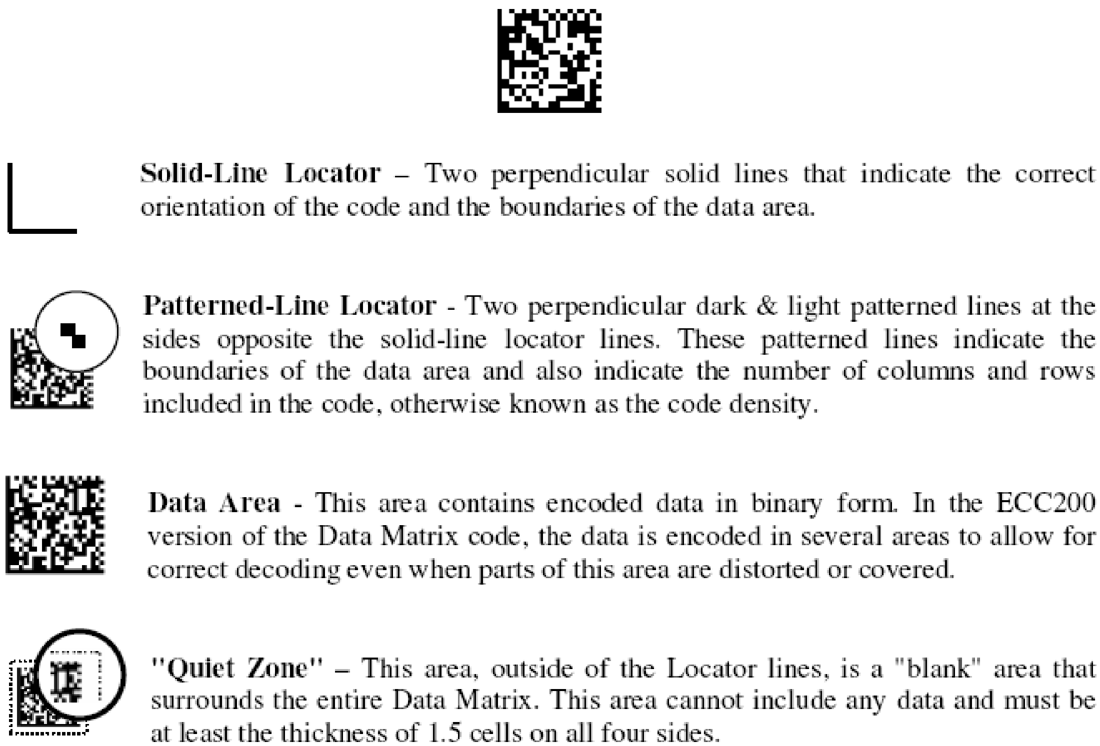
Another advantage of 2D systems over 1D is its durability. An additional stripe at the beginning or at the end of a 1D will easily create an error in reading. The scanner can errantly read a character just by a mere increase in the width of any of the stripes in the bar code. A 2D bar code has been proven to resist read errors caused by pinholes, additional ink markings and tearing.

3. UID and the 2D Matrix

Both UID technology and symbology have migrated from the single one-dimensional bar code to a 2D bar code system. The 2D bar code system utilizes a two-dimensional matrix as shown in Figure 6. The 2D matrix is accepted world-wide and complies with both MIL STD-130[19] and the International Organization for Standardization (ISO).

[19] MIL STD-130 requires that all qualifying end item deliverables, government furnished property in possession of contractors, and legacy items be marked with a 2D Data Matrix bar code.

Figure 6. Two-Dimensional Matrix[20]



The most commonly used 2D symbologies are PDF417, DataMatrix, MaxiCode and the QR Code. Both PDF417 and DataMatrix have storage capacities of 2,000 characters. They are both designed to carry an entire data file which can be extracted with a portable reader. The most common uses of PDF417 and DataMatrix are for logistics and transportation, retailing, healthcare, identification and manufacturing.

The two other symbologies were developed for more specialized purposes. MaxiCode was created by United Parcel Service (UPS) and was designed to ensure accuracy in the scanning of packages on fast moving conveyors. MaxiCode has a storage capacity of 93 data characters, the symbols are composed of a central bulls-eye locator combined with off-set rows of hexagonal elements. The QR Code was developed in

[20] 2D Matrix Barcodes White Paper. (2005). Retrieved on November 7, 2007, from http://www.visidot.com/files/2D_Data_Matrix-White_Paper.pdf.

Japan and can encode up to 1,500 alpha-numeric characters. The design of the block codes allow for expansion in size to carry more information.

4. Marking

UID is a system that identifies an item from manufacture to disposal. The challenge arises from how to ensure that the 2D matrix that represents each item stays with that item throughout its life-cycle. To accomplish this, the UID may be applied to an item using one of three methods: label, data plate or direct part marking. Figure 7 depicts several examples of 2D matrixes used to mark items.

Figure 7. 2D Matrix Part Marking[21]

Dot Peen Ink Jet Label Laser Engraved Tesa Tape

5. Database

The use of UID on an item has no value without a database registry. The UID Registry maintained by Defense Logistics Information Service (DLIS) is “the ultimate repository where all UID data will be captured and stored.” The registry information about each item that is maintained in the database will include: what the item is, its original owner, its initial value, acceptance timing, and any other information deemed

[21] IUID toolkit. (2007). Retrieved on November 7, 2007, from http://www.iuidtookit.com.

pertinent. To transmit UID data to the registry for new items, the Wide Area Work Flow Receipt and Acceptance (WAWF-RA)[22] process will be used.[23]

6. Scanning

The 2D matrix scanners that will be used to capture the UID information and ultimately interface with the registry are also a step beyond the technology used for the 1D bar code. Specifically, the 2D matrix scanners use high-resolution, image capturing technology vice the 1D bar code scanners use of optics that measure the intensity of the reflected light. The advantage of image capturing is that the 2D matrix can be read at various angles and orientations compared to the 1D scanners. Another advantage is that some 2D matrix scanners also incorporate the 1D scanning technologies making the same device useful for transitioning to the new technology.

7. The UID System

Putting together all of the technology: the 2D matrix, the part marking, the database and the scanners, provides a system that will lead to improvements and efficiencies within DoD asset management. As shown in Figure 8, the UID system begins at production with product marking and submission to the UID registry. At that point, the item is uniquely identified among all of the assets within DoD's vast inventory and will lead to achieving the stated goals of DoD:

> UID is a Department of Defense program that will enable easy access to information about DoD possessions and will make acquisition, repair, and deployment of items faster and more efficient. [24]

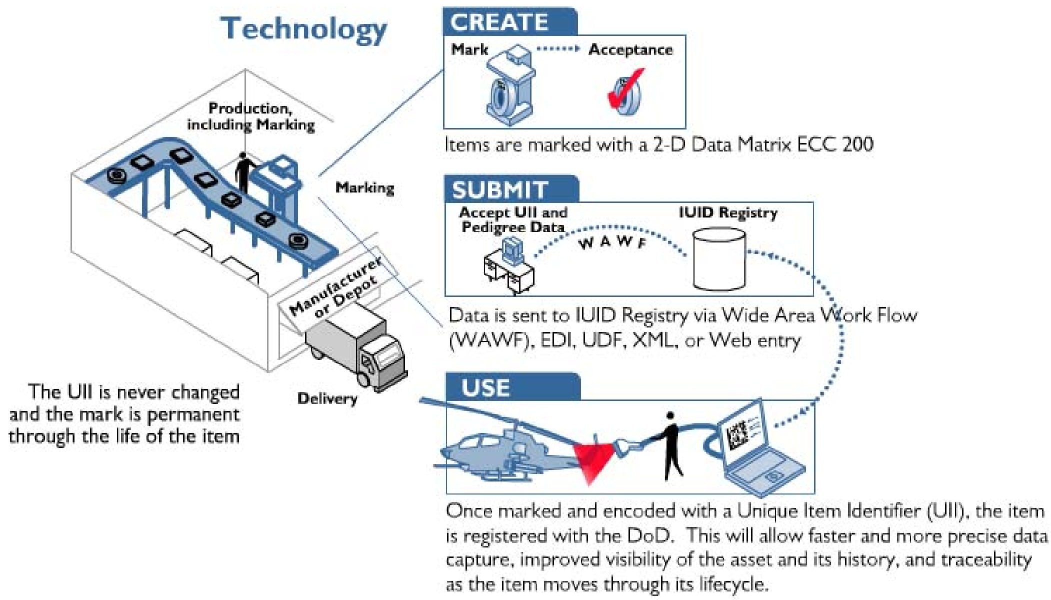
---

[22] According to the Defense Finance and Accountability web site, Wide Area Work Flow - Receipts and Acceptance (WAWF-RA) is a Paperless Contracting DoD-wide application designed to eliminate paper from the receipts and acceptance process of the DoD contracting lifecycle.

[23] IUID toolkit. (2007). Retrieved on November 7, 2007, from http://www.iuidtookit.com.

[24] Defense Procurement and Acquisition Policy. Retrieved on November 7, 2007 from http://www.acq.osd.mil/dpap/pdi/uid/index.html.

Figure 8. UID Technology[25]



B. HISTORY OF UID

The history of UID compared to RFID is much shorter, though no less significant in its development. For the purposes of this project the history of UID covers the period from introduction to the DoD mandate for UID's implementation. Significant events that occurred after the mandate will be covered in a later section.

1. Origins

In 1987, the first two-dimensional (2D) bar code symbol was designed and perfected by David Allais of the Intermec Corporation.[26] Assigned the name, Code 49,

[25] IUID toolkit. (2007). Retrieved on November 7, 2007, from http://www.iuidtookit.com.

[26] 107 Adams Communications. Bar code-1 2-Dimensional Bar Code Page. Retrieved on August 22, 2007, from http://www.adams1.com/pub/russadam/stack.html.

the new symbol held significantly more data than the traditional 1D bar code by utilizing between two to four rows of 1D bar codes stacked on top of each other.[27]

Siemens Corporation, made the final leap to UID in 1989 with its invention of the 2D Data Matrix symbol. The Siemens data matrix incorporated 2D matrix code with a capacity of 500 characters per symbol.[28] The 2D matrix and the required computer system to read and record the information stored in the matrix are called Unique Item Identification.

2. Development

In the late 1990s and early 2000's, UID utilization began all over the world and especially in the retail and supply chain management sectors of business. Merchandise such as soda cans, packaged groceries, repair parts, appliances, and large equipment, was labeled with 2D data matrix symbols. These UID symbols stored large amounts of information about the product and its history that could be quickly accessed and recorded by readers and computers.

As of January 1, 2004, UID system implementation became mandatory on all Department of Defense procurement contracts for a significant amount of materials and equipment as directed by the Under Secretary of Defense, Acquisition, Technology, and Logistics (USD AT&L).

[27] 107 Adams Communications. Bar code-1 2-Dimensional Bar Code Page. Retrieved on August 22, 2007, from http://www.adams1.com/pub/russadam/stack.html.

[28] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. NAVY RFID AND UID

A. OVERVIEW AND POLICY[29]

The Navy RFID and UID programs have developed in response to the Department of Defense policies that directed each DoD component to prepare plans for each AITs separate implementation.

1. DOD RFID Policy

The DoD policy has three parts:

- Immediate implementation of the active RFID data-rich tag to meet Combatant Commander (COCOM) ITV (In-Transit Visibility) requirements.
- Adoption of innovative RFID technology for use at the case/unit level to optimize supply chain management.
- The Supplier Implementation Plan that describes the parameters and the schedule for DoD suppliers to use passive RFID tags (USN RFID Implementation Plan, 2).

In order to develop an implementation plan that conforms to the DoD policy and addresses all three of the policy's parts, the Navy is focusing upon two key concepts, "central management" and "phased implementation."

Central Management will ensure that the effort and expenditure of Navy resources will be consolidated in the navy AIT Program Office. All RFID standards and equipment will be approved centrally with particular regard to the initial roll-out phase. During the

[29] Parts of this section are drawn from Department of the Navy. (2005). United States Navy Radio Frequency Identification (RFID) Implementation Plan.

initial roll-out, all software and hardware requirements will be identified by individual commands and then centrally collected for budgeting and execution of initial procurements by the AIT office. Individual commands will then be responsible for life-cycle management and upkeep while the AIT office maintains responsibility for upgrades and submits the budget to Naval Supply Systems Command (NAVSUP). Phased Implementation will be the prioritization of selected systems and platforms that will allow the Navy to maximize utility while minimizing the investment and operational risks associated with implementation.

2. DoD UID Policy

On July 29, 2003 the acting USD (AT&L), Michael W. Wynne, issued a memorandum detailing the mandatory requirement for the DoD to incorporate UID on "all solicitations issued on or after January 1, 2004."[30] According to Mr. Wynne, the implementation of UID throughout the DoD is an initiative that will "enhance logistics, contracting and financial business transactions."[31] It will also allow the department to capture the value of the items that it procures, manage those items throughout their life-cycle and simultaneously provide a means to prevent counterfeiting of parts.[32]

The memorandum specifically stated that UID would be used for all government property delivered after January 1, 2004 if it met any of the following criteria:

- The acquisition cost is $5,000 or more.
- The item is serially managed, mission essential, controlled inventory or a repairable or consumable item that requires permanent identification.

[30] Department of Defense, Office of the Under Secretary of Defense (Acquisition, Technology and Logistics). (July 29, 2003). Memorandum. Policy for Unique Identification (UID) of Tangible Items - New Equipment, Major Modifications, and Reprocurements of Equipment and Spares.

[31] J. Kann, (2004) Navy Supply Corps Newsletter. Understanding Unique Identification. Jan-Feb 2004, pp. 1-4.

[32] Ibid.

- The item is a component of a delivered item that the program manager has determined requires UID.
- A UID (or DoD recognized equivalent) is available.[33]

The policy emerged from a UID Integrated Product Team (IPT) that was comprised of members from "DoD Finance, Acquisition, Logistics, Information Management, DoD Components, Joint Staff, Industry and International communities."[34]

The IPT's goal was to develop data standards and business rules as well as an implementation strategy that could bring UID to the DoD as quickly as possible. The IPT divided the UID project into three phases: Phase I - Requirements, Phase II - Implementation/Migration Planning, and Phase III - Outreach and Communication.

Phase I, Requirements, was completed in April of 2004 and was marked with an agreement on the data elements that would constitute a UID. Phase II, Implementation, has been moving forward and will require several years for completion.

3. NAVSUP/Navy AIT Office

The Chief of Naval Operations, Director, Supply, Ordnance and Logistics Operations Division (OPNAV N41) is the functional sponsor for Navy AIT. OPNAV N41 has directed the NAVSUP to manage and operate the Navy AIT Program Office. The Navy AIT Program Office is located at Mechanicsburg, Pennsylvania and works with the designated AIT representatives within the 35 Echelon II commands and other key elements. The mission of the Navy AIT Office is to "foster a community of

[33] Department of Defense, Office of the Under Secretary of Defense (Acquisition, Technology and Logistics). (July 29, 2003). Memorandum. Policy for Unique Identification (UID) of Tangible Items - New Equipment, Major Modifications, and Reprocurements of Equipment and Spares.

[34] J. Kann, (2004) Navy Supply Corps Newsletter. Understanding Unique Identification. Jan-Feb 2004, pp.1-4.

understanding through the participation, definition, resolution, and dissemination of AIT related standards, technologies, and implementation issues."[35]

The AIT programs that are managed out of the Program Office include:

- Navy Serial Number Tracking (SNT)
- Navy Common Access Card (CAC)
- Publicizing UID policy; UID program and hardware education.[36]
- Navy Radio Frequency Identification (RFID) Implementation [37]

Table 4 shows the Navy AIT Program Office Summary of Actions demonstrating the Office's role in the Navy AIT Implementation Plan.

Table 4. Roles of the Navy AIT Program Office[38]

Action	Lead Organizations	Coordinating Organizations	Completion Date
RFID hardware and unique software requirements shall be identified for all commands and submitted to Navy AIT Program Office when identified.	Navy Echelon II Commands	Navy AIT Program Office	Continuing
Search for ITV gaps and will identify future investment requirements accordingly.	Navy TAV Office	Navy AIT Program Office	Continuing
Assist OPNAV, and OSD Supply Chain Integration and RFID Office's working groups to resolve issues and determine appropriate courses of action.	Navy AIT Program Office	Navy AIT Program Office	Continuing
Report plan implementation progress measurements semiannually to the Navy AIT Program Office.	Navy Echelon II Commands	Navy AIT Program Office	Semi-annually as directed
Develop detailed progress reporting guidance.	NAVSUPSYSCOM	Navy AIT Program Office	4th QTR FY06
Adopt specific measurement metrics	NAVSUPSYSCOM	Navy AIT Program Office	Continuing
Coordinate with the Navy AIT Program Office when taking significant action in response to the plan requirements, particularly when developing or upgrading AISs that will be RFID-enabled.	Echelon II Commands and AIS Owners	Navy AIT Program Office	Continuing
Conduct liaison with Hardware Systems Commands (HSCs), PM J-AIT, supporting vendors and activities/units to coordinate efforts to equip in support of the ITV effort	NOLSC/NAVSUP	Navy AIT Program Office	Continuing

35. J. Kann, (2004) Navy Supply Corps Newsletter. Understanding Unique Identification. Jan-Feb 2004, pp.1-4.

36 Ibid.

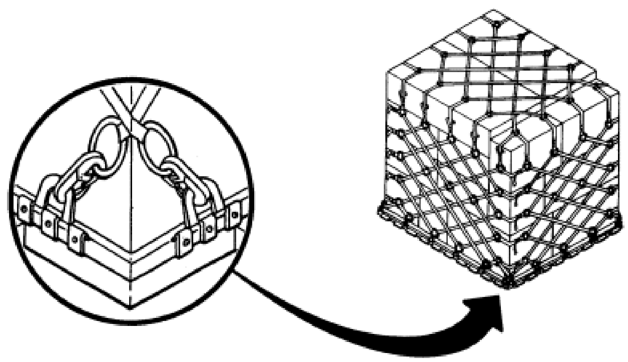
37 Navy AIT Technology Office. Automatic Identification Technology/Radio Frequency Identification. Retrieved on June 12th, 2007, from, http://www.palm.saic.com/ait.htm.

38 Ibid.

B. NAVY’S SUPPORT OF RFID POLICY

The first part of the DoD RFID Policy is the use of active RFID to meet COCOM requirements. Specifically, the COCOMs require that the tag can be used on a freight container such as the 463L pallets with net as shown in Figure 9.

Figure 9. 463L Pallet.



The Navy fully supports this policy for ITV, but seeks to minimize investment in permanent infrastructure that would exceed the COCOMs requirements unless the Navy can achieve a positive ROI. The Navy’s preference is for the use of mobile equipment, such as Portable Deployment Kits (PDKs) and Early Entry Deployment Support Kits (EEDSKs) pictured in Figure 10, which can more easily be used on a contingent basis.[39]

Figure 10. Portable Deployment Kits

[39] Department of the Navy. (2005). United States Navy Radio Frequency Identification (RFID) Implementation Plan. p.3.

The second part of the policy involves the use of passive RFID. Adoption of passive RFID's goal is to optimize the supply chain providing the highest ROI and creating cost savings. An AIT Project Office Business Case Analysis recommended deferring major passive RFID investments until POM 08 (FY08-FY13) allowing for further evaluation and technological development. One of the ongoing evaluations is at the Trident Refit Facility in Bangor, Washington which will allow for the assessment of passive RFID and the validation of the Navy's ROI calculations. [40]

The third and final part of DoD's policy is the Supplier Implementation Plan. DoD has described this policy as delivering a "truly transformational technology that will play a vital role in achieving the DoD vision for implementing knowledge-enabled logistic support to the war fighter through fully automated visibility and asset management."[41] In compliance with this policy, as of October 1, 2004, the Navy has mandated passive RFID tag use on solicitations issued for delivery of material on or after January 1, 2005.[42]

C. NAVY'S RFID GOALS AND OBJECTIVES

The Navy's overall objectives as listed in the Navy's RFID Implementation Plan include:

- Develop and initiate RFID implementations that add value to Navy logistics processes in a standard fashion, balancing effectiveness and efficiency. Focus will be on ROI/cost savings and contribution to readiness.

---

[40] Navy Passive RFID Business Case Analysis presentation. (May 8, 2007). Retrieved on November 10, 2007, from http://www.dla.mil/j-6/ait/Files/Conferences/Supply_Chain_Vis_Forum/Tuesday/T-5.%20%20Navy%20AIT%20Update.pdf.

[41] Department of Defense. (2007). United States Department of Defense Suppliers' Passive RFID Information Guide, Version 9.0.

[42] R. L. Gaiser Jr., & C. Hunt, From Acquisition to Distribution: Human Systems Integration in the Supply Chain.

- Integrate RFID into all applicable logistics processes and related Automated Information Systems (AISs).
- Achieve Total Asset Visibility (TAV) throughout the entire supply chain using RFID as an enabler.
- Focus on RFID implementation that will enhance supply processes (e.g. receipt, stow, inventory and issue).[43]

These objectives outline the Navy's plan in response to the USD (AT&L)'s memorandum stating the DoD policy for RFID. The Navy's push to achieve these objectives has manifested in several initiatives.

D. NAVY'S RFID AND UID INITIATIVES

1. Active RFID

One active RFID initiative to meet the requirements of the COCOMs is the outfit of Fleets and component commands with deployable active RFID capability to support contingent operations. The outfitting of three EEDSKs, plus one set (1200) of tags to Commander, Fleet Forces Command (CFFC) in support of contingencies will be available as "standby deployable assets" under the control of the Naval Operations Logistics Support Center (NOLSC). Additional kits will be procured for CENTCOM, EUCOM, PACOM, and SOUTHCOM AOR's. An estimated total of 15 kits in all will be procured by the NOLSC who will also be in charge of delivery with training and maintenance performed by the NAVSUP/Navy AIT Office.[44]

The Navy is also using active RFID tags on jet engine/module containers that are shipped to both CONUS and OCONUS sites that include afloat units and non-self deploying units. In accordance with DoD policy, the Navy will affix active RFID tags to

[43] Department of the Navy. (2005). United States Navy Radio Frequency Identification (RFID) Implementation Plan. p. 3.

[44] Department of the Navy (2006). Navy Active RFID/In-Transit Visibility Concept of Operations (CONOPS). pp.8-9.

those containers, which number an estimated 8,000 containers. Out of those 8,000 containers, an estimated 3,200 are being shipped between OCONUS sites per year. The goal is to use the COCOM tagging requirements to track the jet engine/module containers when in storage as well as in-transit. An additional use of the tags will be to continuously monitor the humidity levels and environmental conditions that these tags are exposed to providing additional data benefits. These initiatives are only a few of the active RFID programs that are currently in development and implementation by the Navy.

2. Passive RFID

The Navy has started several RFID supply chain implementation initiatives at a variety of locations for both passive and active RFID. In 2003, the Navy's Fleet and Industrial Supply Center (FISC) Ocean Terminal Division in Norfolk, Virginia, implemented a passive RFID inventory control system.[45] The Ocean Terminal Division receives less-than-container load shipments from various sources and consolidates them into oceangoing containers for export to forward deployed forces.[46] The passive RFID system is used to generate manifests that are electronically written to a tag attached to the container, to control consolidation, and to validate container contents.[47]

A second passive RFID initiative was designed to substantiate the results from the Navy's Business Case Analysis (BCA) for passive RFID. The BCA findings demonstrated that further study was required to determine the best use of passive RFID as an enabling technology for both global fleet freight warehouse and pier side operations and that the ROI would not be realized until five years after implementation at ashore installations. Some specific recommendations that emerged from the BCA were:

- Defer major passive RFID investments until POM 08

---

[45] U. M. Apte, N. Dew, & G. Ferrer, (2006). What is the Right RFID for Your Process? *Acquisition Research Sponsored Report Series*. p.27.

[46] Ibid.

[47] A. F. Estevez, & S. Geary, (2006). RFID: The Future is Now. *Exceptional Release*. p.28.

- Select key business process targets to analyze and process data for use in the future.
- Influence standards to support the Navy's requirements.

The initiative to evaluate the BCA findings is an on-going "focused implementation" at the Trident Refit Facility in Bangor, Washington known as the Bangor RFID Evaluation (BRE). [48] The BRE was meant as a means to facilitate the decision-making process for future RFID implementation and to substantiate the results from the Navy's BCA. This initiative is expected to significantly improve the supply chain processes of stocking, warehouse refusal, inventory accuracy and to significantly impact customer wait time. The Navy also expects that the BRE will validate the preliminary ROI predictions for ashore installations.[49]

3. RFID and UID

The Navy has moved forward with its initiatives on both passive and active RFID, but the real value can be realized when both AITs are combined into one system. At the Naval Surface Warfare Center Carderock Division, Philadelphia (NSWC Carderock), passive RFID technology is used in conjunction with UID and Contact Memory Buttons (CMB) in its Total Asset Configuration – Visibility and Tracking (TAC-VAT) system. This system is integrates logistic material, data, management and workforces into one system that delivers complete access and visibility. The authors have identified the NSWC Carderock system as a useful model for an RFID and UID wireless network plan.[50]

Another initiative that is also combining RFID implementation with UID is that of SPAWAR San Diego. It was during a site visit to SPAWAR that the authors were

---

[48] Department of the Navy. (2005). United States Navy Radio Frequency Identification (RFID) Implementation Plan, p.3.

[49] Ibid.

[50] R. L. Gaiser Jr., & C. Hunt, From Acquisition to Distribution: Human Systems Integration in the Supply Chain.

demonstrated a Navy Supply Chain warehouse AIT system that could be used as a model for future concurrent RFID and UID implementations, which we discuss in the next chapter.

V. SPAWAR CONCURRENT RFID AND UID IMPLEMENTATION

A. OVERVIEW

SPAWAR performs the mission of delivering FORCEnet[51] to the Navy. It is dedicated to inventing, acquiring, developing, delivering and supporting "integrated & interoperable command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), business IT and space capabilities in the interest of national defense."[52] As part of the C4ISR development, the SPAWAR San Diego Field Activity, SSC San Diego, has eight formal leadership areas as directed by the Assistant Secretary of the Navy (Research, Development and Acquisition). One of those formal leadership areas is Command, Control and Communications.

B. SATCOM SHOP

At SSC San Diego, one of the Departments within the Command, Control and Communications leadership areas is Fleet Engineering. Fleet Engineering provides "expertise across the full spectrum of integrated C4ISR, from prototype implementation through systems engineering and support of fielded systems. Within Fleet Engineering, is the Extremely High Frequency (EHF) Satellite Communications (SATCOM) Branch Code 4122 which "provides a full range of engineering, management and logistics services in support of the EHF SATCOM Programs for the U.S. Navy."[53] Code 4122 has

[51] FORCEnet is "the operational construct and architectural framework for Naval Warfare in the Information Age that will integrate WARRIORS, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force, scalable across the spectrum of conflict from seabed to space and sea to land." Source: http://forcenet.navy.mil.

[52] Command Information. (n.d.). Retrieved on September 27, 2007, from Space and Naval Warfare Systems Command:.http://enterprise.spawar.navy.mil.

[53] Extremely High Frequency (EHF) Satellite Communications (SATCOM). (2007). *Special Capabilities and Services.* Jones, B.: Author.

put into place a concurrent implementation of RFID and UID technologies as a means for supply chain management process improvement.

1. Background

The implementation of the concurrent RFID and UID at Code 4122 was initiated in response to the DoD mandates, the process requirements within SPAWAR, and to improve the efficiency of its current processes. The stated goals for the use of RFID/UID by Code 4122 are:

- Maximize efficiencies of life-cycle asset management with integration of RFID/UID throughout DoD.
- Leverage technology to improve the ability to get the customer the right materiel, at the right time, and in the right condition.
- The technology is critical to the End-to-End War fighter Support initiative.[54]

Prior to implementation, Code 4122 faced difficulties that could be considered typical of warehouse-based operations. The manual processes that were involved in the areas of inventorying, shipping, receiving and maintenance were prone to human error and time-consuming inefficiencies.

2. Pre-implementation Processes

The inefficiencies that were identified in Code 4122 centered on the processes of receiving and inventorying.[55] In particular, the receiving process involved several manual steps that were prone to human error, as follows.

[54] Y. Y. Wong, & B. Jones, (2007, March). Using RFID and IUID to Reduce Life Cycle Costs Lessons Learned. Presentation.

[55] Y. Y. Wong, & B. Jones, (2007, March). Introduction to Machine Readable Information. Presentation.

a. Receiving

- All received parts are placed in a stack.
- The packing list is placed on a clipboard for manual verification.
- One part at a time is counted, verified against the packing list and moved to a separate stack.
- Occasionally during the inventory process the person that is doing the inventory may be interrupted.
- If the last part on the pallet does not match the last part on the packing list, then the person doing the inventory will have to count the parts again.
- Once the parts have been verified, the part numbers are hand typed into a configuration management database and the parts are placed in a specified location.[56]

b. Inventorying

Code 4122 currently has over 17,000 line items of inventory both within configurations and on shelves that is valued at over $150 million. The Inventory Integrity procedures at SPAWAR San Diego require that high dollar value items, those greater than $1,000 in value, have an inventory accuracy of 99%. Those inventories can consist of either quarterly spot checks or annual wall-to-wall inventories. That is, if the results of the quarterly spot checks are less than the required 99%, then a wall-to-wall inventory must be conducted.[57]

---

[56] Y. Y. Wong, & B. Jones, (2007, March). Introduction to Machine Readable Information. Presentation.

[57] Ibid.

The pre-implementation inventory process, like the receiving process, is also hampered by manual processes and prone to errors. An example that illustrated this point is how the consolidation of like numbered parts, but unlike readiness condition (RFI vice NRFI), stored in the same location could lead to improper inventory counts using a manual process.[58] An improper inventory count could then hinder the level of customer service to the fleet.

c. Pre-implementation Lessons Learned

The lessons learned were that both the receiving and inventorying processes were slow because of manual inputs that were also prone to errors. Miscounts during the inventories caused delays and the database entries were susceptible to typographical errors of wrong part numbers, serial numbers and location entries.[59] It was determined that the way to reduce human error and the time-consuming processes was to adopt the machine readable information technology that could be found in concurrent implementation of RFID and UID.

3. Post-Implementation Processes

The processes that are now in place within Code 4122 all use a Supply Chain Management System called Catalog Ordering Logistic Tracking System (COLTS) that manages the information generated by the RFID/UID systems. COLTS allows for export and import of information between all the AIT devices.[60] RFID and UID are now integral to the inventorying, shipping, receiving and maintenance processes that are conducted on a daily basis.

---

[58] Y. Y. Wong, & B. Jones, (2007, March). Introduction to Machine Readable Information. Presentation.

[59] Ibid.

[60] Ibid.

a. Inventory

Figures 11 and 12 depict the inventory processes and the use of the AIT systems. The processes are divided between materiel stored in rack and bins and materiel that resides within equipment.

Figure 11. Inventory in Racks and Bins[61]

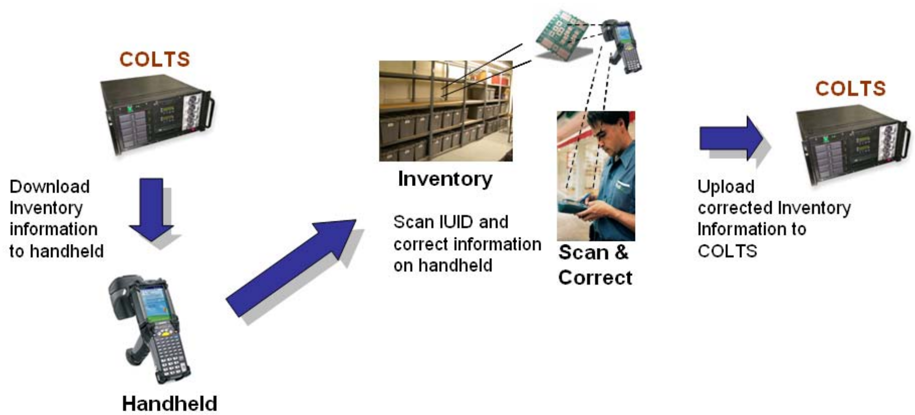
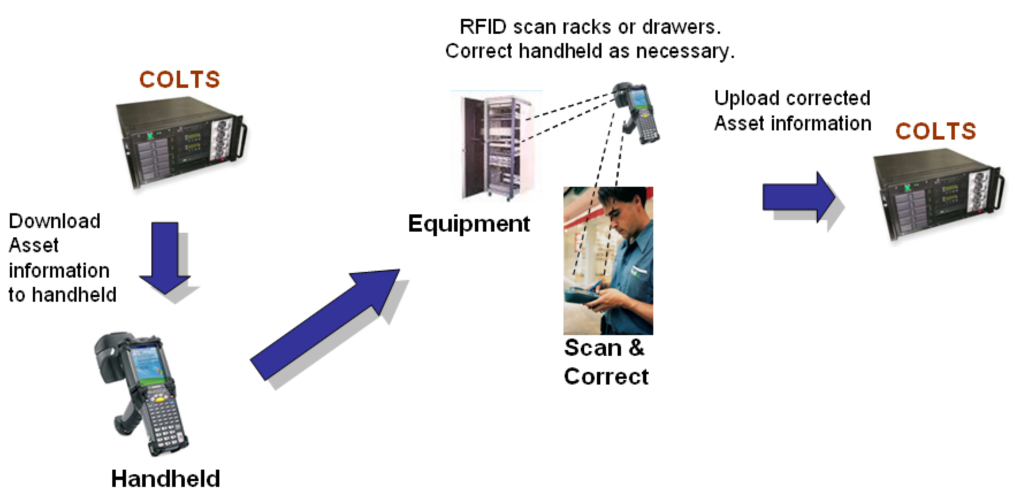


Figure 12. Inventory Assets Inside Equipment[62]



[61] Y. Y. Wong, & B. Jones, (2007, March). Introduction to Machine Readable Information. Presentation.

[62] Y. Y. Wong, & B. Jones, (2007, March). Using RFID and IUID to Reduce Life Cycle Costs Lessons Learned. Presentation.

b. *Shipping*

As depicted in Figure 13, the shipping process originates with a pick list that is generated by the COLTS system. The requested part is pulled from inventory, the inventory is updated, and the part is delivered to the shipping area. At the shipping area the AIT devices, either handheld or portal readers, automatically send scanned information back to COLTS. COLTS then generates the shipping document.

Figure 13. Shipping[63]

c. *Receiving*

As shown in Figure 14, receiving begins where all material received is processed using handheld scanners or portal readers depending on the presence of RFID, UID or a standard bar code. The material is then affixed with a local tag that has both RFID and UID and then placed in the appropriate warehouse location. Simultaneously COLTS is updated to reflect the receipt.

---

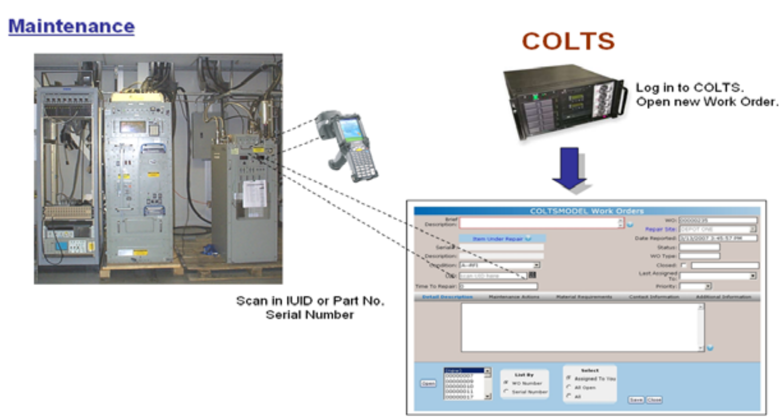
63 Y. Y. Wong, & B. Jones, (2007, March). Using RFID and IUID to Reduce Life Cycle Costs Lessons Learned. Presentation.

Figure 14. Receiving[64]

d. Maintenance

The final process utilizing AIT systems that is performed by Code 4122 is maintenance. As shown in Figure 15, components and individual parts are scanned using handheld scanners into the COLTS system. The system automatically generates the work order to perform the required maintenance.

Figure 15. Maintenance[65]



[64] Y. Y. Wong, & B. Jones, (2007, March). Using RFID and IUID to Reduce Life Cycle Costs Lessons Learned. Presentation.

[65] Ibid.

4. Success at SPAWAR

The implementation of RFID and UID at Code 4122 resulted in significant cost avoidance. As shown in Table 5, the inventory cost difference, over a range of 100 parts, yielded $120.35 per part. This difference is attributable to the reduction in the amount of time required for each process. Table 6 further shows that the reductions would yield significant total cost avoidance over a five-year period. These cost avoidances are a direct result to a reduction in labor. The authors' purpose for discussing this data is to show that the efficiencies gained in the processes allow for resources, both time and money, to be reallocated to other areas and does not necessarily require or result in a reduction in the labor force.

Table 5. Inventory Cost Differences per Part.[66]

Inventory Cost Differences Per Part

Between using MRI with Handheld and human data entry

Method	# of Parts	Labor$/Hr	Labor$/Min	# of Minutes	$/Part
Manually	100	$50	$0.83	150	$124.50
Handheld	100	$50	$0.83	5	$4.15
SAVINGS PER PART					**$120.35**

[66] Y. Y. Wong, & B. Jones, (2007, March). Using RFID and IUID to Reduce Life Cycle Costs Lessons Learned. Presentation.

Table 6. RFID/UID Cost Analysis for the Inventory Process.[67]

Naval Extremely High Frequency Satellite Program (NESP) UID/RFID Cost Analysis Consulting Team: PEO C4I Consulting In Cooperation with SPAWAR System Center Code 2622, Barry Jones						
Without RFID and IUID:						
Yearly Total Costs/Hours for Five Years						
	Year 1	Year 2	Year 3	Year 4	Year 5	**Total**
Cost	$109,833.33	$109,833.33	$109,833.33	$109,833.33	$109,833.33	**$549,166.67**
Hours	2622	2622	2622	2622	2622	
With RFID and IUID:						
Yearly Total Costs/Hours for Five Years						
	Year 1	Year 2	Year 3	Year 4	Year 5	**Total**
Costs	$38,565.73	$23,035.73	$23,035.73	$23,035.73	$23,035.73	**$130,708.67**
Hours	450	450	450	450	450	
Avoidance:						
Total Cost Avoidance						
	Year 1	Year 2	Year 3	Year 4	Year 5	**Total**
Costs	$71,267.60	$86,797.60	$86,797.60	$86,797.60	$86,797.60	**$418,458.00**
Hours	2,172	2,172	2,172	2,172	2,172	

67 Y. Y. Wong, & B. Jones, (2007, March). Using RFID and IUID to Reduce Life Cycle Costs Lessons Learned. Presentation.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RFID/UID CONCURRENT IMPLEMENTATION

A. NSWC CRANE

1. Background

NSWC Crane is the third largest Navy installation in the world. Located in Crane, Indiana, NSWC Crane employs over 2,700 personnel and its facilities encompass a 100 square mile area. NSWC Crane is a multi-mission, multi-service, product center that supports both fleet and industrial customers.[68] NSWC Crane's mission is to provide low-cost, quality, and responsive acquisition, in conjunction with superior logistics and maintenance support to the Navy's weapons and electronics systems.[69] Within the overall structure of NSWC Crane, the major supply support and inventory management operations are conducted in the central supply warehouse located in Building 41.

2. Research and Analysis of Current Operations

a. Inventory Management System

The primary inventory management system used at the NSWC Crane warehouse Building 41 is the Industrial Logistics Support Management Information System (ILSMIS). ILSMIS is a 25-year-old legacy system that was recently rewritten in Oracle and rolled out in May, 2007. The system supports most logistics processes including procurement and requisition, warehouse/inventory management, maintenance, distribution and disposal. The system comprises at least 266 tables, and its hard copy data element dictionary is 385 pages long. Crane manages over 73,000 individual line items with a total depth of 12.4 million components.

---

[68] Who We Are, Command and Mission Statement. (n.d.). Retrieved on November 9, 2007 from Naval Surface Warfare Center Crane Division: http://www.crane.navy.mil/whoweare/.

[69] Ibid.

The results from the initial site survey visit and subsequent opportunities to review ILSMIS documentation show that the new Oracle upgrade to ILSMIS has actually institutionalized some last generation material management and inventory processes, i.e. paper-based manual input methods of material control. For example, in order to conduct an inventory, personnel are required to print inventory cards and then manually count and annotate the material and quantity counted on the card. These inventory cards are then used to manually enter the inventory figures back into ILSMIS to verify quantity and location of materials. An inventory report is then produced by ILSMIS which includes a discrepancy listing. A lengthy, manual reconciliation process is required as there are both actual and counting errors that must be investigated.

Another example of a paper-based action is the material receipt process. Upon receipt of material, the document number and tracking number are recorded on a receipt document that is carried to an ILSMIS client PC and manually input via keyboard. These processes do not take advantage of the latest advances in AIT such as RFID or UID.

b. Locally Generated Systems

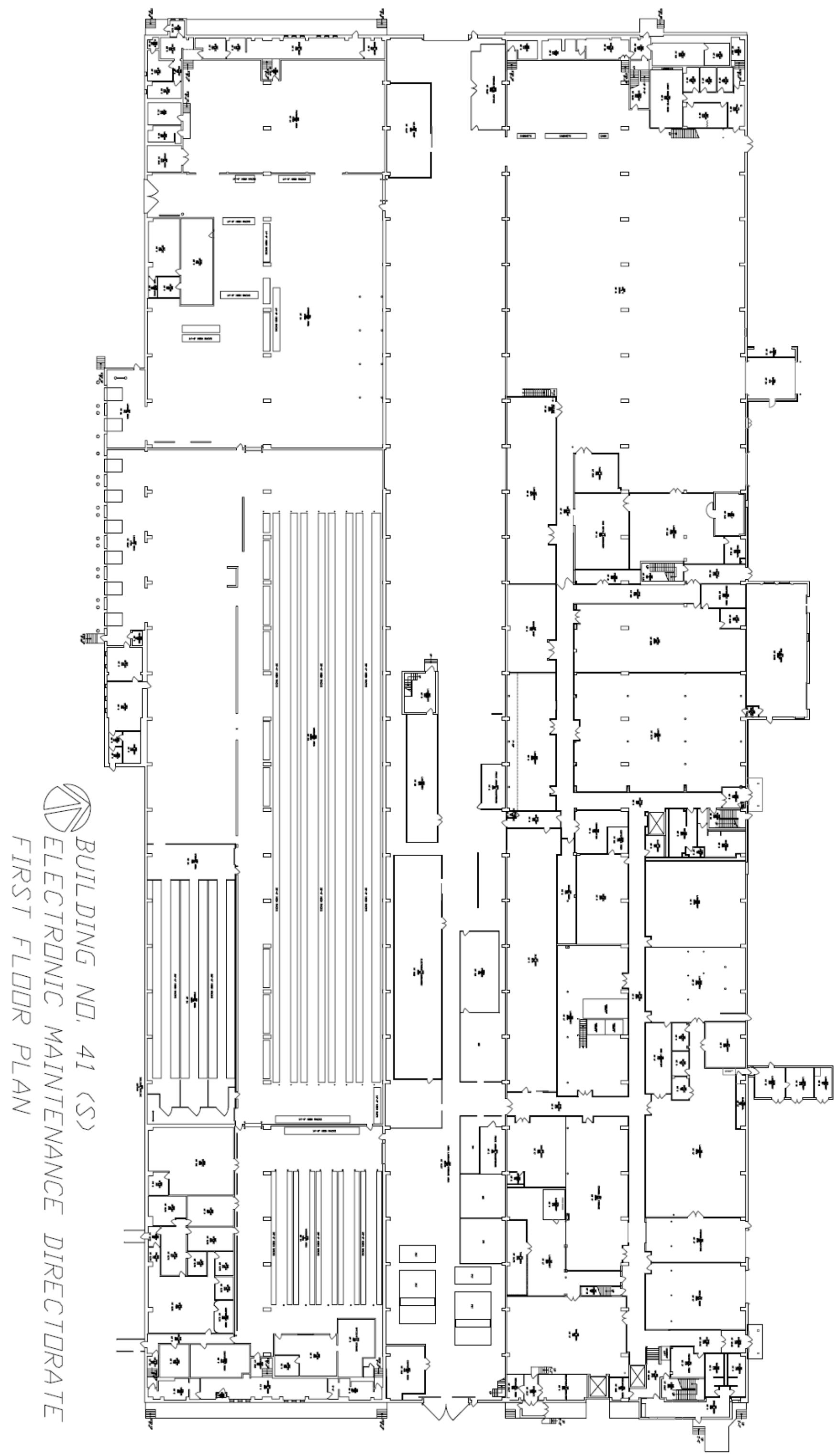
There are also other locally generated systems that are used to supplement the inventory and tracking capabilities of ILSMIS. Delivery Tracking System (DTS) is a stand-alone Access database used to track packages and pallets from the receiving area in building 41 to other areas within the building and to other warehouses or maintenance shops. This system utilizes bar code and scanner technology.

In addition to DTS there is a small, stand alone database that is used to track firearms by serial number within the firearms warehouse and maintenance buildings. The stand-alone system is used in parallel with ILSMIS as is able to incorporate serial numbers to identify each individual piece of weaponry.

c. *Facility Description*

Building 41 is the central warehouse for logistics operations at Crane. Building 41 is the focus of our research and analysis. The space is not environmentally controlled and the floor area is approximately 817,000 sq ft. Building 41 is equipped with Local Area Network connectivity, power, lighting and the location of the ILSMIS database. Figure 16 shows the floor plan of Bldg 41.

Figure 16. Warehouse Building 41



d. Material Tracking

The types of materials currently managed and tracked in building 41 of NSWC Crane are of two types: serially managed and bulk items. Serially managed for designated organizations such as the Aegis Program Office or Naval Inventory Control Point (NAVICP) include unique items such as electron tubes, circuit card assemblies, and power supplies. Bulk items, which are sponsor owned material, are managed using both National Stock Number (NSN) and/or Part Number

e. Material Marking

Stored materials are marked using linear bar codes that consist of the Document Number, NSN, and Serial Number. Two types of software, Bartender and Loftware, are used to create 2" x 4" and 4" x 6" labels for boxes. Certain Department Codes also use hand written Inspection tags on some specific material that moves through their shops. Materiel that has been repaired by Crane maintenance shops is affixed with linear bar codes. NSWC Crane does not create UID labels at this time; however, UID labels are affixed to some material received from suppliers such as DLA. For shipping purposes, NSWC Crane personnel utilize ILSMIS to create PDF 417 bar codes on DD1348 documentation.

f. Processes

Material management processes involve receiving, stowing, inventory, issuing, packaging, cross-docking, and shipping. Currently these processes are very labor intensive. At each step in the movement of material, personnel write Document Number, NSN or Part Number data onto a piece of paper and then manually enter the information into a computer, with many opportunities for error.

B. RFID/UID CONCURRENT IMPLEMENTATION ROLL-OUT PLAN

1. Overview

a. Functional Description

The NSWC Crane RFID/UID concurrent implementation system that will result from this project is NSWC Crane Inventory Management System (NCIMS) Wireless Complex. NCIMS will include four separate staging areas that receive and process material. All of the leading edge RFID portals, the wireless, handheld RFID and UID scanners, the printers, and the special software associated with these devices will be utilized, evaluated and accredited. The devices will use a web-based Oracle application to store the data and the latest DoD compliant encryption system in order to protect the transmission of the wireless information.

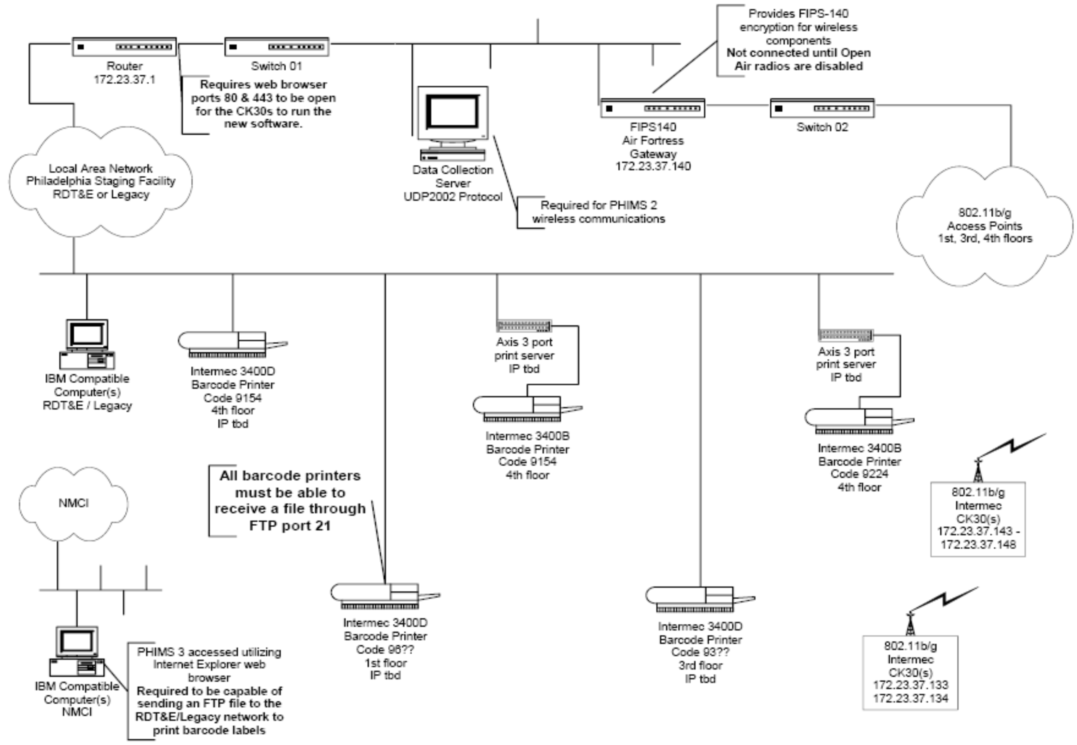
The steps provided in the following implementation plan integrate the basic phases of the NSWC Carderock wireless network plan and our acquisition and installation recommendations developed through research and site visits to SPAWAR San Diego and NSWC Crane.

b. Wireless Network System Architecture

The approved system architecture developed by NSWC Carderock for the Philadelphia Inventory Management System (PHIMS) Wireless Complex incorporates the basic concepts and fundamentals required by the Navy to operate a secure wireless network. These same concepts and fundamentals is used to design the system architecture of NCIMS. The authors recognize the differences in facility and location characteristics between NSWC Crane and NSWC Carderock. Therefore, it must be understood that the PHIMS architecture provides only the foundation and general plan for building the NCIMS architecture plan. The NCIMS architecture and network is modified to meet specific requirements at NSWC Crane as determined by the NSWC Crane leadership management. Naval Network Warfare Command (NETWARCOM) and the

Navy AIT Office must approve the NCIMS system architecture plan prior to implementation and operation. The System Security Authorization Agreement (SSAA) for the NSWC Carderock PHIMS Wireless Complex[70] describes the operations of NSWC Carderock and illustrates the system architecture utilized by the PHIMS. Figure 17 illustrates the topology of the PHIMS that is used as a model in designing NCIMS.

Figure 17. Functional Overview of PHIMS Topology[71]



[70] The SSAA is a single source document for all information pertaining to the certification and accreditation processes for operating a Department of the Navy wireless inventory management system.

[71] Naval Surface Warfare Center Carderock Division System Security Group. (2006). *System Security Authorization Agreement for Philadelphia Inventory Management System Wireless Complex.* Philadelphia, PA: U.S. Government Printing Office.

2. Implementation Roles and Responsibilities[72]

Portions of this section are directly excerpted from the SSAA for NSWC Carderock in order to maintain the integrity and intent of the original document.

a. Designated Approving Authority (DAA)

The DAA is responsible for evaluating the mission, business case analysis, and budgetary needs for the system in view of the security risks. The DAA is also responsible for the making the decision to formally grant Approval to Operate thus accepting the residual risk.

b. Certification Authority (CA)

The Certification Authority will:

- Approve security requirements.
- Review and approve the Certification and Authorization (C&A) process tailoring and level-of-effort determination.
- Oversee C&A security evaluations.

c. Certification Agent Representative

The Certification Agent Representative will:

- Evaluate threats, vulnerabilities and risks.
- Sign the certification package.
- Prepare the accreditation package for the DAA to review and sign.

[72] Parts of this section are drawn from Naval Surface Warfare Center Carderock Division System Security Group. (2006). *System Security Authorization Agreement for Philadelphia Inventory Management System Wireless Complex.* Philadelphia, PA: U.S. Government Printing Office.

d. Certification Team

The Certification Team will provide guidance on issue resolutions, policy adherence, and system analysis with respect to security.

e. Information Assurance Manager (IAM)

The Information Assurance Manager (IAM) for NSWC Crane is the focal point for Information System Security Policy and Guidance and coordinates with the DAA and Chief Information Officer (CIO) to ensure that C&A is accomplished for all information systems in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The IAM is responsible for the implementation of the Information Assurance (IA) Program at NSWC Crane. Additional responsibilities for the IAM include the following:

- Act as the focal point for all IA policy and monitor its implementation. Coordinate with the chain of command.
- Develop the Information Assurance Program (IAP). Approve all deviations from and inform the DAA prior to approval of any deviation to the IAP.
- Ensure appoint of the Information System Security Staff in writing and coordinate appointments with the chain of command.
- Obtain DAA signature on Memorandum of Agreements (MOAs) prior to connecting command Information Systems (i.e. LANs, WANs, Metropolitan Area Networks (MANs), stand-alones, and laptops) to any external information systems.
- Obtain authority from the DAA to operate information systems prior to implementation. A determination of an acceptable level of risk will form the basis for requesting authority to operate the system.

- Ensure security violations are investigated and expeditiously resolved. Approve solutions within the IA policy. If necessary, deny access to affected systems. Inform the DAA via the chain of command of actions taken.
- Ensure that virus attacks are resolved and reported to Navy Certified Incident Response Team (NAVCIRT).
- Ensure that computer network attacks/intrusions are reported expeditiously to NAVCIRT per Computer Network Incident Reporting Procedures.
- Review command On Line Surveys for documented vulnerabilities, plan, coordinate, and apply corrective actions to minimize vulnerabilities to an acceptable level of risk.
- Ensure an effective procedure is in place to handle Information Assurance Vulnerability Alerts (IAVA) and Information Condition (INFOCON) compliance and reporting.

f. NCIMS Administrator (NCIMS-A)

The NCIMS-A will direct the development, operations and maintenance of the NCIMS, define and manage the NCIMS schedule and budget, and work with the CA to reach an agreement on all critical security issues for the system. The NCIMS-A is also the primary operational network security individual and is responsible for the execution and completion of the SSAA under the Information System Security Policy and Guidance provided by the IAM. Additional responsibilities include:

- Act as the focal point for all command LAN (Unclassified and/or classified) and associated network components.
- Ensure that C&A is maintained and up-to-date for NCIMS

- Conduct periodic checks to verify compliance with existing Information System Security policy/procedures and ensure that safeguards are maintained. Monitor command information system activity and review existing audit trails. Provide recommendations to correct problem areas and improvements concerning the SSAA or Risk Management processes to the command IAM.
- Document, evaluate, and report all security risks and violations to the command IAM. If the situation warrants and the IAM is not readily available, shut down or deny access to systems. Promptly inform IAM and chain of command of actions taken.
- Ensure Standard Operating Procedures (SOPs) affecting the IA environment are created and properly implemented.
- Ensure annual review and execution of all SOPs to ensure enforceability and applicability to the current environment.

The NCIMS-A will liaise with SPAWAR Code 4122 via NAVSUP-FISC AIT Office for system topology design, hardware, software, and installation recommendations. The NCIMS-A will provide updated implementation status to the NSWC Crane Supply Officer and the Navy AIT Office via NAVSUP-FISC AIT staff.

3. NSWC Crane RFID/UID Implementation Team

In addition to the NSWC Crane personnel that are directly involved, the RFID/UID Implementation Team is a partnership built from multiple outside organizations and groups with significant experience and knowledge in both logistics and AIT. This collective experience and knowledge of the team provides the best path to successful implementation and operation of AIT.

a. COMFISCS AIT Office

The COMFISCS Logistics Automation Manager, Ms. Jane Zimmerman, has formed a multi-organizational team called the UID Implementation team. The UID Implementation team's tasking is to implement AIT across Systems Commands (SYSCOMS) in support of the Navy's Material Support Integration (MSI). The partners associated with this venture are Naval Air Systems Command (NAVAIR), Naval Sea Systems Command (NAVSEA), Naval Facilities and Engineering Command (NAVFAC) Commander Navy Installations Command (CNIC) and SPAWAR.

b. SPAWAR Systems Command Code 4122

Led by Mr. Y.Y. Wong and Mr. Barry Jones, SPAWAR Code 4122 is a Navy leader in RFID/UID implementation. The RFID/UID system developed and utilized by Code 4122 provided the baseline guidance for NSWC Crane's concurrent RFID/UID implementation. Code 4122 will provide detailed instruction with regards to system hardware and integration.

c. Applied Enterprise Solutions

Applied Enterprise Solutions (AES) is the contractor hired by the Commander Fleet and Industrial Supply Centers (COMFISCS) AIT Office to integrate the RFID/UID middleware with the current ILSMIS network at NSWC Crane. Mr. Bill Henley is the head of project development.

d. Naval Postgraduate School Supply Chain Logistics Group

The Naval Postgraduate School Supply Chain Logistics Group, "Team Monterey", is a team of Naval Supply Officers consisting of LCDR Ernan Obellos, LCDR Ryan Lookabill, and LCDR Travis Colleran, authors of this report. The team is advised by Dr. Geraldo Ferrer, Dr. Nick Dew, and Dr. Thomas Housel.

4. Implementation Phases

The Implementation requires four phases. Phase 1: Preparation, Phase 2: Refinement of System Security Authorization, Phase 3: Acquisition and Installation of NCIMS components, and Phase 4: Final Approval. Tables 7, 8, 9 and 10 at the end of each phase show a breakdown of tasks, points of contact (POC) and estimated labor required for implementation completion.

a. Phase 1: Preparation

This phase lays the foundation for building the NCIMS network. It documents the system vision, mission, candidate materials, and desired end-state. Additionally, this phase defines all of the DoD wireless network and information assurance and compliance requirements that must be accomplished prior to implementation.[73] For Crane's implementation, the following candidate materials are identified:

- Items valued at greater than $5,000
- Serially managed (unique items): repair parts, plant property
- Bulk Sponsor Owned Material (NSN or Part Number): repair parts and bulk materials

[73] Administrative compliance requirements are further addressed in the NSWC Carderock SSAA.

Table 7. Phase 1: Preparation[74]

Task Description	POC	Labor Required
Phase – 1 Preparation • Document mission need. • Determine and document mission functions. Conduct registration • Prepare mission description and system identification. • Prepare environmental and threat description. • Prepare system architecture description. • Determine the certification level. • Determine the system security requirements. • Identify the organizations that will support the Certification and Administration (C&A) • Tailor the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) task, determine the C&A scope, man-hour required, and prepare the DITSCAP plan. • Develop the draft System Security Authorization Agreement (SSAA) • Conduct (MSCL)	System Security Group (SSG) NCIMS-A	100 hrs
Approved security concepts. • Concur with stated security concepts	DAA User Rep CA IAM	10 hrs

b. Phase 2: Refinement of System Security Authorization Agreement

This phase builds on the products created during the preparation phase. It involves analysis and development of system architecture and software design. During

[74] Naval Surface Warfare Center Carderock Division System Security Group. (2006). *System Security Authorization Agreement for Philadelphia Inventory Management System Wireless Complex.* Philadelphia, PA: U.S. Government Printing Office.

this phase, NSWC Crane AIT personnel will liaise and collaborate with the COMFISCS contracted software developer, AES, to integrate the current inventory management software, ILSMIS, with the front-end RFID/UID software. NCIMS will utilize a specific software package that will consist of software components loosely coupled around a service-oriented architecture. Logic functions will be published as Service Oriented Architectural Protocol (SOAP)[75] web services in order to ease the integration of the existing ILSMIS software and to promote flexibility.

Since the system logic and workflow are implemented via SOAP web services, user interfaces may be implemented in a variety of technologies. Bar code readers and external software systems will be integrated on a case-by-case basis. This architecture is built for integration of ILSMIS, R-Supply[76], and with RFID/UID technology. According to Mr. Bill Henley of AES, "It is also well prepared to include other technologies when opportunities present themselves."[77] This phase will also include the tag specifications decision.

[75] Naval Surface Warfare Center Carderock Division System Security Group. (2006). *System Security Authorization Agreement for Philadelphia Inventory Management System Wireless Complex.* Philadelphia, PA: U.S. Government Printing Office.

[76] R-Supply is the Navy's Supply Management system which handles all inventory, financial and logistics functions in support of fleet operations.

[77] B. Henley, personal communication, October 16, 2007.

Table 8. Phase 2: Refinement of System Security Authorization Agreement[78]

Task Description	POC	Labor Required
Phase – 2 Refine the SSAA. Support system development activities. Perform certification analysis. • System architecture analysis. • Software design analysis. • Network connection rule compliance analysis. • Integrity of integrated products analysis. • Life-cycle management analysis. • Vulnerability assessment analysis. Design of tags to be used Assess analysis results against SSAA requirements. Draft Security Test & Evaluation (ST&E) Plan.	 NCIMS-A CA IAM SPAWAR Code (4122)	50 hrs

c. *Phase 3: Acquisition and Installation of NCIMS Components*

Acquisition of hardware, software, materials and services for installation will be solicited to the open market. Criteria for fair and reasonable pricing will be determined by the contracting officer in compliance to Defense Federal Acquisition Regulation Supplement (DFARS) and the specifications as determined by SPAWAR. Cost-effective, reliable, and compliant RFID and UID hardware products are readily available for purchase.[79] Additional guidance is provided in the NSWC Carderock SSAA.

[78] Naval Surface Warfare Center Carderock Division System Security Group. (2006). *System Security Authorization Agreement for Philadelphia Inventory Management System Wireless Complex.* Philadelphia, PA: U.S. Government Printing Office.

[79] Contact SPAWAR Systems Command, Code 4122, Mr. Y.Y. Wong, wongyy@spawar.navy.mil or Mr. Barry Jones of Northrop Grumman Ship Systems, barry.jones@ngc.com for detailed instructions with regards to software and hardware procurement and integration.

Installation of the RFID/UID system to the NCIMS is a service contract to be determined by the contracting officer. The installation service contractor will work side-by-side with AES for front-end software integration with ILSMIS. Scheduling and other details will be promulgated by the NCIMS Data Base Administrator (NCIMS-DBA) who is in charge of the overall installation, evaluation and life-cycle maintenance of the system. NCIMS-DBA will report plan implementation progress measurements to the Navy AIT Program Office[80].

80 This recommendation is added in order to comply with the directive in Navy RFID Implementation Plan, published on December 8, 2005.

Table 9. Phase 3: Acquisition and Installation of NCIMS Components[81]

Task Description	POC	Labor Required
Phase – 3 Acquisition of system hardware, software & tags • Contact SPAWAR Systems Command San Diego, CA for recommended hardware IAW system architecture and software design analysis. • COMFISCS and AES will provide middle-ware and software specifications IAW system architecture and software design analysis. • Contact SPAWAR Systems Command, San Diego, CA for recommended RFID/UID tag specifications applicable to NSWC material candidates. • Contact SPAWAR Systems Command, San Diego, CA for recommended job scope description for system installation Consolidate and submit all requirements to NSWC Contracting Office for purchase actions. Install and integrate RFID/UID system and front-end software system with ILSMIS	SPAWAR Code (4122) NCIMS-A CA IAM Contracting Officer AES Installation Contractor	120 hrs

d. Phase 4: Final Approval

Final refining and certification along with approval for operation of NCIMS will be granted by NETWARCOM and the Navy AIT Office. This milestone will be the responsibility of NCIMS-DBA.

[81] Naval Surface Warfare Center Carderock Division System Security Group. (2006). *System Security Authorization Agreement for Philadelphia Inventory Management System Wireless Complex.* Philadelphia, PA: U.S. Government Printing Office.

Table 10. Phase 4: Final Approval[82]

Task Description	POC	Labor Required
Phase – 4 Finalize the SSAA Certification evaluation of the integrated system. • Implement the ST&E • (If application does not comply with IA Controls outlined in DoD 8500.2: pursue IATO; provide methods of mitigation; & return to Phase – 2) • Run system scan (i.e., penetration testing). • Analyze and document test results. • Conduct system and risk-based management analysis review. • Contingency plan evaluation. Develop recommendation to DAA. DAA accreditation.	 NCIMS-A CA IAM	40 hrs
Approval to operate • Draft and route an ATO for DAA's signature.	IAM	10 hrs

5. Training

Per the Navy RFID Implementation Plan, the DoD Logistics AIT Office has been tasked to develop a multi-level RFID/UID education and training plan for use by all Navy organizations and agencies. The NCIMS-DBA will contact the DoD Logistics AIT Office to determine the proper training program to educate personnel. The NCIMS-DBA

[82] Naval Surface Warfare Center Carderock Division System Security Group. (2006). *System Security Authorization Agreement for Philadelphia Inventory Management System Wireless Complex.* Philadelphia, PA: U.S. Government Printing Office.

will then conduct training classes for all users prior to granting access to the system. Data base security and personnel proficiency are the goals for an efficient RFID/UID operation.

C. IMPLEMENTATION SUMMARY

The total estimated labor required for implementation is 330 hours. This equates to 41.25 full work days for planning, meeting administrative requirements, the acquiring and installation of equipment and software and the startup of the NCIMS network. Implementation time variables can be expected during the certification, acquisition and installation phases and should be planned for accordingly.

VII. KVA AND ROI FOR CONCURRENT RFID AND UID IMPLEMENTATION AT NSWC CRANE

A. INTRODUCTION

Accurate metrics for assessing the rate of return of public funding investments, along with the operational readiness benefits received, are critical given increased regulations and requirements for enhanced accountability and transparency. The latest example of those requirements is the DoD Directive 8115.01 issued October, 2005 mandating the use of performance metrics based on outputs with ROI analysis required for all current and planned IT investments.[83]

Our study is based on the work "Integrated Portfolio Analysis: Return on Investment and Real Options Analysis of Intelligence Information Systems (Cryptologic Carry on Programs)" by LCDR Cesar G. Rios Jr., Dr. Thomas Housel and Dr. Jonathan Mun of the Naval Postgraduate School. They applied the Knowledge Value Added (KVA) framework to estimate the ROI on IT investments with an analytical tool set that also supports strategic, performance-based investment decisions.[84] KVA methodology, to derive ROI valuation, is used in this section to conduct a business case analysis of the concurrent RFID/UID implementation at NSWC Crane.

B. RETURN ON INVESTMENT

Historically, DoD programs resulted in cost overruns due to extended delivery schedules as a consequence of erroneous time and money estimates.[85] As a result, an accurate determination of ROI on DoD IT development programs has remained elusive for decades. Although to the same degree as DoD, the private sector has experienced the

---

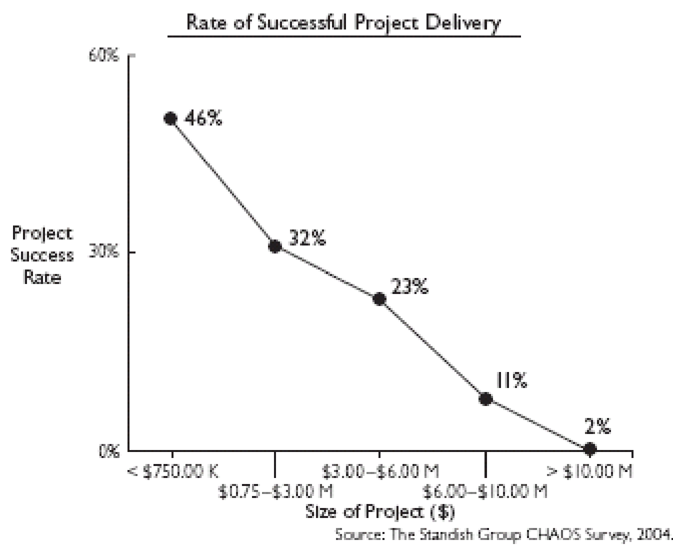
[83] C. Rios, T. Housel, & J. Mun,, (2006). Integrated Portfolio Analysis: Return on Investment and Real Options Analysis of Intelligence Information Systems (Cryptologic Carry On Program). Naval Postgraduate School. p.4.

[84] Ibid.

[85] Ibid.

same challenges with large technology projects having a dismal success rate. Figure 18 below, from the research firm The Standish Group, depicts a 68% failure rate of IT projects with \$3 million and above invested.[86]

Figure 18. Rate of Successful IT Project Delivery[87]



1. Measuring ROI in the Private Sector

With a high probability of failure rate the private sector has developed rigorous tools to measure the benefits from IT investment with various methods created to capture an accurate value of ROI. The corporate-level focuses on the value-added from human capital and IT assets to the overall performance, while the sub-corporate-level used output-input ratios of their core processes. Other methodologies use financial measures and estimates to quantify a heuristic approach. Despite differences in approach and

[86] C. Rios, T. Housel, & J. Mun,, (2006). Integrated Portfolio Analysis: Return on Investment and Real Options Analysis of Intelligence Information Systems (Cryptologic Carry On Program). Naval Postgraduate School. p.2

[87] Ibid.

methodologies, the end-state is to provide the decision makers with a measurement of the value for IT investments.[88] Table 11, shows the different approaches in measuring ROI for IT.

[88] C. Rios, T. Housel, & J. Mun,, (2006). Integrated Portfolio Analysis: Return on Investment and Real Options Analysis of Intelligence Information Systems (Cryptologic Carry On Program). Naval Postgraduate School. p.3.

Table 11. Approaches to Measuring Return on IT[89]

Level of Analysis	Approach	Focus/Assumptions	Key Advantages	Limitations
Aggregate Corporate (firm) level	*Process of Elimination (i.e. Knowledge Capital)*	• Treats effect of IT on ROI as a residual after accounting for other capital investments	• Uses commonly accepted financial analysis techniques and existing accounting data	• Cannot drill down to effects of specific IT initiatives • ROI on IT difficult to measure directly
	Production Theory	• Determines IT effects through input output analysis using regression modeling techniques • Economic production function links IT investment input to productivity output	• Uses econometric analysis on large data sets to show contributions of IT	• "Black-box" approach with no intermediate mapping of IT's contributions to outputs
	Resource-Based View	• Links firm's core capabilities with competitiveness • Uniqueness of IT resource = competitive advantage	• Uses strategic advantage approach to IT impacts	• Causal mapping between IT investment and firm competitive advantage difficult to establish
Corporate/ sub-corporate	*Option Pricing Model*	• Determines best point to exercise an option to invest in IT • Timing exercise option = value	• Predicts future value of IT investment	• No surrogate for revenue at sub-corporate level
Sub-corporate (Process) level	*Family of Measures (i.e. Balanced Scorecard)*	• Measures multiple indicators to derive unique contributions of IT	• Captures complexity of corporate performance	• No common unit of analysis/ theoretical framework • Multiple indicators required to measure performance
	Cost-Based (i.e. Activity-Based Costing)	• Uses cost to determine value of IT • Derivations of cost ≈ value	• Captures accurate cost of IT	• No surrogate for revenue at this level; no ratio analysis
	Knowledge Value Added (i.e. KVA)	• Allocates revenue to IT proportionate to contributions to process outputs • IT contributions to output ≈ IT value-added	• Allocates revenue and cost of IT allowing ratio analysis of IT value-added	• Not directly applicable to highly creative processes

89 P. Pavlou, T. Housel, W. Rodgers, & E. Jansen,. (July 2005). "Measuring the Return on Information Technology: A Knowledge-Based Approach for Revenue Allocation at the Process and Firm Level," Journal of the Association for Information Systems, Vol. 6, No.7, pp.199-226

2. The Difference between the Private Sector and DoD

Most ROI measures focus solely on financial returns that are not applicable for measuring returns of DoD IT investment. In DoD's business, an IT investment is expected to increase the overall operational readiness of the war-fighters, which is not measurable in monetary form. As previously mentioned, this study utilizes the KVA methodology in order to quantify the value-added in operational readiness language when the RFID/UID system is implemented.

C. THE KVA VALUATION FRAMEWORK AND OVERVIEW

The KVA valuation framework does not only provide metrics for operating performance, cost-effectiveness and return on investments, but it can also incorporate portfolio management techniques to value programs. KVA can also take into account uncertainty and risk in estimating future benefits.

The DoD applicability of KVA is focused on the outputs of core processes and sub-processes which provide several products or benefits to include:[90]

- Common units of output that quantifies value of specific processes and functions of departments, divisions, or organizations.
- Historical data of cost and revenues of specific processes.
- Emphasizes operational efficiencies/inefficiencies within all levels of analysis all the way to individual employees and IT system.
- Uses other portfolio investments by estimating the potential total value created.

[90] C. Rios, T. Housel, & J. Mun,, (2006). Integrated Portfolio Analysis: Return on Investment and Real Options Analysis of Intelligence Information Systems (Cryptologic Carry On Program). Naval Postgraduate School. p.4.

In the private sector, the KVA framework can be used to obtain the value of the company from specific divisions to individual employees and systems to determine profitability. Organizations can quantify the value of specific processes and their contribution to the bottom line with the KVA framework. DoD services can utilize the framework to optimize existing performance tools.

D. KVA METHODOLOGY

The KVA methodology process is summarized in Table 12. This includes the general data collection process guidelines according to Rios, Housel and Mun.

Table 12. NPS Valuation Framework[91]

Data Collection	**KVA Methodology**
• Collect baseline data • Identify sub- processes • Research market comparable data • Conduct market analysis • Determine key metrics	**Step 1**: Calculate time to learn. **Step 2**: Calculate value of Output (K) for each sub-processes. **Step 3**: Calculate Total K for process. **Step 4**: Derive Proxy Revenue Stream. **Step 5**: Develop the Value Equation Numerator by assigning revenue streams to sub-processes. **Step 6**: Develop value equation denominator by assigning cost to sub-processes. **Step 7,8,9**: Calculate metrics: Return on Investment (ROI) Return on Knowledge Assets (ROKA) Return on Knowledge Investments (ROKI)

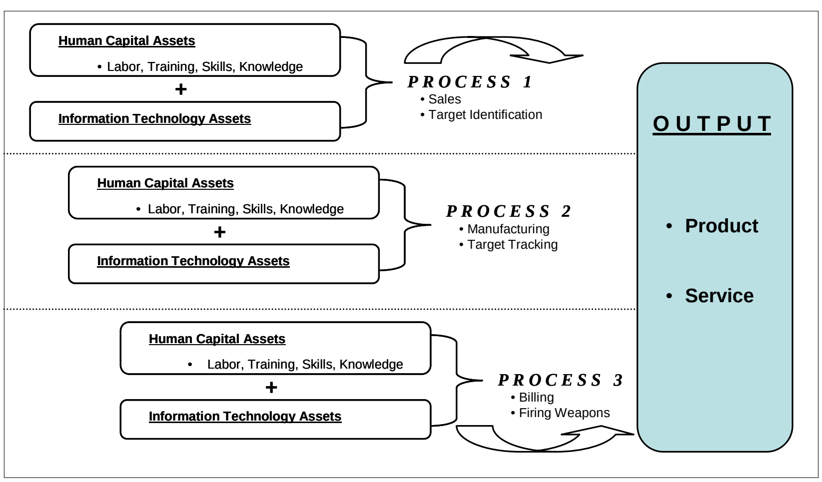
91 C. Rios, T. Housel, & J. Mun,, (2006). Integrated Portfolio Analysis: Return on Investment and Real Options Analysis of Intelligence Information Systems (Cryptologic Carry On Program). Naval Postgraduate School. p.5.

Data collection on identified processes and sub-processes needed to create a "widget" is the first step. A widget is simply defined as a unit of output. This step is then supplemented with a market comparison on cost and revenue to establish a baseline. The value and cost for each process is then estimated using the KVA methodology. The final step is the ROI analysis, which uses the data from cost per unit to produce a "widget" and the "widget" price per unit estimates.

As previously mentioned, KVA quantifies the value provided by human capital and IT assets of specific processes at all levels. This provides a picture of each dollar invested in IT by monetizing the outputs of all assets, including intangible, knowledge assets.

KVA identifies the actual cost and revenue of a product or service by isolating the value of knowledge embedded in an organization's core processes, employees and IT. As emphasized by Rios, Housel and Mun, KVA identifies every process required to produce an output. It identifies the historical costs of those processes, the unit costs and calculates the unit prices of products and services. An output is defined as the end result of an organization's operations; it can be a product or service as shown in Figure 19.[92]

Figure 19. Measuring Output[93]



[92] C. Rios, T. Housel, & J. Mun,, (2006). Integrated Portfolio Analysis: Return on Investment and Real Options Analysis of Intelligence Information Systems (Cryptologic Carry On Program). Naval Postgraduate School.p.6.

[93] Ibid.

For the past fourteen years, KVA has been used in over 100 organizations in both public and private sectors with employees ranging from 20 to thousands. Within DoD, the methodology has been applied in 35 areas, ranging from flight scheduling, ship maintenance and modernization processes.[94] As a performance tool used by the DoD, the KVA methodology has been used to:

- Compare all processes in terms of relative productivity
- Allocate revenues to common units of output
- Measure value added by IT by the outputs it produces
- Relate outputs to cost of producing those outputs in common units
- Provide common unit measures for organizational productivity[95]

Based on the tenets of complexity theory, KVA assumes that humans and technology in organizations add value by taking inputs and changing them into outputs through core processes.[96] The amount of change an asset or process produces can be a measure of value or benefit. Additional assumptions in the KVA methodology include:

- Describing all process outputs in common units (i.e., the time it takes to learn to produce the required outputs) allows historical revenue and cost data to be assigned to those processes at any given point in time.
- All outputs can be described in terms of the time required to learn how to produce them.
- Learning Time, a surrogate for the knowledge required to produce process outputs, is measured in common units of time. Consequently, Units of Learning Time = Common Units of Output (**K**).

---

[94] C. Rios, T. Housel, & J. Mun,, (2006). Integrated Portfolio Analysis: Return on Investment and Real Options Analysis of Intelligence Information Systems (Cryptologic Carry On Program). Naval Postgraduate School., p.7.

[95] Ibid.

[96] T. Housel & A. Bell, Measuring and Managing Knowledge. Boston: McGraw-Hill, 2001. pp. 92-93.

- Common unit of output makes it possible to compare all outputs in terms of cost per unit as well as price per unit, because revenue can now be assigned at the sub-organizational level.
- Once cost and revenue streams have been assigned to sub-organizational outputs, normal accounting and financial performance and profitability metrics can be applied.[97]

Describing processes in common units also permits to generate market-comparable data, which is particularly important for a non-profit organizations such as the DoD. Market-comparable data from the commercial sector can be used to estimate price per common unit, allowing for revenue estimates of process outputs for non-profits. This also provides a common basis to define benefit streams regardless of process analyzed. As demonstrated in Table 13, KVA differs from other ROI models because it allows for revenue estimates enabling use of traditional accounting, financial performance and profitability measures.[98]

Table 13. Comparison of Traditional Accounting versus Process Based Costing

Explains what was spent

Traditional Accounting		KVA Process Costing	
Compensation	$5,000	Review Task	$1,000
Benefits/OT	1,000	Determine Op	1,000
Supplies/Materials	2,000	Input Search Function	2,500
Rent/Leases	1,000	Search/Collection	1,000
Depreciation	1,500	Target Data Acq	1,000
Admin. And Other	900	Target Data Processing	2,000
Total	**$11,400**	Format Report	600
		Quality Control Report	700
		Transmit Report	1,600
		Total	**$11,400**

Explains how it was spent

[97] C. Rios, T. Housel, & J. Mun,, (2006). Integrated Portfolio Analysis: Return on Investment and Real Options Analysis of Intelligence Information Systems (Cryptologic Carry On Program). Naval Postgraduate School. p.7.

[98] Ibid, p.8.

KVA can rank processes in terms of the degree to which they add value to the organization or its processes. This capability assists decision-makers to identify what processes add value -- those that will most likely accomplish a mission, deliver a service, or meet customer demand. Value is quantified in four key metrics: Return-on-Knowledge (ROK), Return on Knowledge Assets (ROKA), Return on Knowledge Investment (ROKI) and Return on Investment (ROI).

E. KVA AND ROI APPLICATION TO INVENTORY MANAGEMENT AT NSWC CRANE

1. Measuring Efficiency and Effectiveness

For this study, the KVA methodology was utilized to quantify the value of implementing RFID/UID technology with ILSMIS to form the overall NCIMS Network. Specifically, the efficiency (productivity) and effectiveness (profitability) of the inventory process were measured by comparing the values created by human capital elements and RFID/UID IT elements utilized in inventory functions. The identification of all assets, processes and sub-processes, provides the foundation for the value measurement, quantification and analysis.[99]

The asset analysis includes all values and costs for each asset included in the inventory process. Process outputs are determined by "amount of time to learn" estimates and include the total aggregate process outputs and a revenue stream used to monetize the outputs. The analysis of all sub-processes includes time-to-learn, how-to-perform, and the number of times each sub-process is accomplished.[100]

---

[99] C. Rios, T. Housel, & J. Mun,, (2006). Integrated Portfolio Analysis: Return on Investment and Real Options Analysis of Intelligence Information Systems (Cryptologic Carry On Program). Naval Postgraduate School. p.13.

[100] Ibid.

2. Quantification of KVA Value and Cost Data[101]

Allocation of asset value and cost is distributed within all sub-processes in which a product was contributed. The revenue allocated at the sub-process level was computed by multiplying the "time-to-learn" (embedded knowledge in each sub-process) by the number of personnel involved, the number of times the sub-process was repeated and the market comparable revenue. The revenue allocated at the sub-process level serves as the baseline for revenue allocation.

In this study, the yearly salary of a GS-10, Step 5 employee, was converted to an hourly wage and used to represent the Market Comparable Revenue (MCR) value for each sub-process accomplished by the NCIMS Administrator. This logic was also applied in using the yearly salary of a GS-5, Step 5 employee, to represent the MCR value for each sub-process accomplished by the Inventory Clerk. Summing the values computed for each sub-process leads to the total revenue of the entire inventory process. Multi-year totals are computed by multiplying the total annual revenue by the number of years. Ten years was used in this study to represent the minimum number of NCIMS life-usefulness before obsolescence.

Cost allocated to each sub-process in the inventory process was computed by multiplying the Work Time (actual time performing task) by the number of personnel involved, the number of times the sub-process was repeated and the market comparable cost. The salary rate of a GS-10 Step 5 and GS-5 Step 5 were applied as before to represent the Market Comparable Process Cost (MCPC).

The output of each sub-process in terms of Knowledge Units was calculated by adding the Knowledge Amount Embedded in Information Technology percentage value to the product of estimated learning time (ALT) and the number of employees involved in

[101] Parts of this section are drawn from C. Rios, T. Housel, & J. Mun,, (2006). Integrated Portfolio Analysis: Return on Investment and Real Options Analysis of Intelligence Information Systems (Cryptologic Carry On Program). Naval Postgraduate School. pp.11-13, and T. Housel & J. Barretto, (2008). A Comparable Market Study of RFID for Manual Item-Level Accountability Inventory and Tracking Systems. In K.C. Laudon and J.P. Laudon, Management Information Systems (pp. H-1 – H-15). Upper Saddle River, New Jersey: Prentice Hall.

the sub-process. Total output is computed by summing the Knowledge Units of each sub-process within the overall Inventory Process.

The ROK productivity ratios were computed with Total MCR in the numerator and Total MCPC in the denominator. ROI financial ratios were calculated with MCR minus MCPC in the numerator and MCPC in the denominator.

In order to analyze the benefits of automation in the inventory workflow process, this study compared the current "As Is" inventory process with the recommended "To Be" inventory process. The "As Is" process is a basic, manual inventory operation and the "To Be" process assumes RFID/UID implementation in that inventory operation. The "As Is" and "To Be" inventory sub-processes are listed in Table 14 with the eliminated sub-processes indicated in bold italics.

Table 14. NSWC Crane "As Is" and "To Be" Inventory Sub-Processes

"As Is" Inventory Sub-Processes	**"To Be" Inventory Sub-Processes**
1. SA prints inventory worksheets	1. SA prints inventory worksheets
2. Clerk counts stock items	2. Clerk conducts inventory with handheld device and data is transmitted wirelessly to NCIMS
3. Clerk records count on worksheet	3. SA prints discrepancy report
4. SA manually inputs inventory data into ILSMIS	4. Clerk conducts inventory recount and data is transmitted wirelessly to NCIMS
5. SA prints discrepancy report	5. SA prints final discrepancy report
6. Clerk conducts inventory recount on discrepancies	6. SA prints master inventory report
7. Clerk records recount on worksheet	
8. SA manually inputs recount data into ILSMIS	
9. SA prints final discrepancy report	
10. SA prints master inventory report	

F. ANALYSIS OF WORKFLOW PROCESSES WITH KVA[102]

1. "As Is" Inventory Process Analysis – Current Operations

Analysis of data obtained from the current "As Is" inventory process demonstrates that sub-processes involving the system administrator and ILSMIS technology deliver significant KVA to NSWC Crane operations. However, several of the sub-processes, to include manual inventory counting, recording, and data entry, provide minimal KVA. These sub-processes are less than 51% automated as well as extremely labor intensive. This results in high sub-process costs and minimal ROK and ROI within the overall inventory process. The calculated ROK and ROI for the inventory process is 21.16 percent and negative 78.84 percent using a ten year period as a conservative estimate of the system's useful life[103]. Table 15 illustrates the results of this analysis.

Based on this data analysis, the sub-processes that provide minimal ROK and ROI are potential areas for intelligent automation. In this situation, sub-processes 2, 3, 4, and 8, in Table 15, are steps in the inventory process that can be significantly improved with RFID/UID technology.

2. "To Be" Inventory Process Analysis – Future Operations

The data and calculations in Table 16 show the potential inventory process and sub-processes after RFID/UID implementation. In this situation, the four specific steps identified previously in Table 15 to be weak contributors to ROK and ROI, are replaced by two sub-processes that utilize RFID/UID technology.

Implementation and utilization of RFID/UID technology significantly reduces the labor and time requirements for conducting inventories. The technology also increases the output of the process in the form of more frequent and accurate inventories as seen by

[102] T. Housel & J. Barretto, (2008). A Comparable Market Study of RFID for Manual Item-Level Accountability Inventory and Tracking Systems. In K.C. Laudon and J.P. Laudon, Management Information Systems (pp. H-1 – H-15). Upper Saddle River, New Jersey: Prentice Hall.

[103] Estimate is based upon the current fleet inventory system, RSupply's, life usability which was deployed in 1998.

the increase in the value of Column K, "Total Amount of Knowledge Units." Additionally, the ROK and ROI are dramatically increased. In this example, ROK and ROI grew to 233 percent and 133 percent respectively. As a significant note, the ROI increases from a negative 79 percent to a positive 133 percent. This is a total improvement of 212 percent in ROI.

G. KVA ANALYSIS SUMMARY

The KVA analysis compares the current "As Is" inventory process with the proposed "To Be" inventory process to determine the merits of RFID/UID implementation. The analysis presented demonstrates the benefits of implementation; improved operations efficiency, efficient use of personnel resources, total visibility of warehouse material, and improved customer service.

Within the inventory process there are several sub-processes that are inefficient and very labor intensive. These specific sub-processes contribute little to the overall ROK and ROI of the process. The sub-processes that are weak contributors to the inventory process ROK and ROI are prime candidates to improve process performance with RFID/UID implementation.

As demonstrated in the KVA analysis, implementation of the RFID/UID technology increases output in terms of capability to conduct more frequent and accurate inventories enabling improved asset visibility while also dramatically increasing ROK and ROI. With this gained capability, inventories can be scheduled on a weekly interval to optimize validity and "near-real-time total asset visibility" without straining the warehouse personnel. Additionally, the amount of labor and time required to conduct inventories is significantly decreased. Those manpower gains can be utilized in other areas of operations, such as direct customer service or as decided by management.

.

Table 15. “As Is” Inventory Knowledge Value Added Analysis

Steps	Estimated Learning Time (ALT) (hrs.)	Work Time (hrs.)	Number of Employees	Number of times task completed (Annual)	Sum of task completion (Annual)	Knowledge Amount Embedded in IT (%)	Amount of Knowledge Units (per task)	Total Amount of Knowledge Units (Annual)	% Total Knowledge	Market Comparable Revenue	Total Market Comparable Revenue (Annual)	Process Cost	Total Process Cost (Annual)	ROK
	A	B	C	D	E = A*C*D	F	G = (A*C)+F	H = E*G	I = G/TotalG	J	K = E*J	L = B*J	M = E*L	N = J/L
1) NCIMS-A prints inventory worksheets by location	1	0.25	1	14	14	90.0	91	1274	18%	$27.53	$385	$6.88	$96.36	400%
*2) Clerk conducts inventory of items	1	8	12	14	168	0.0	12	2016	2%	$16.50	$2,772	$132.00	$22,176	13%
*3) Clerk records count on worksheet	0.5	8	12	14	84	0.0	6	504	1%	$8.25	$693	$66.00	$5,544	13%
*4) NCIMS-A manually inputs worksheet data into ILSMIS	1	3	1	14	14	50.0	51	714	10%	$27.53	$385	$82.59	$1,156	33%
5) NCIMS-SA run exception report of missing items	1	0.15	1	14	14	90.0	91	1274	18%	$27.53	$385	$4.13	$57.81	667%
6) Clerk conducts recount	0.5	2.5	12	14	84	0.0	6	504	1%	$8.25	$693	$20.63	$1,733	40%
7) Clerk records recounts on worksheet	0.25	1	12	14	42	0.0	3	126	1%	$4.13	$173	$4.13	$173	100%
*8) NCIMS-A manually inputs data from recount worksheet	1	1	1	14	14	50.0	51	714	10%	$27.53	$385	$27.53	$385	100%
9) NCIMS-SA prints final inventory discrepancy report	1	0.1	1	14	14	90.0	91	1274	18%	$27.53	$385	$2.75	$38.54	1000%
10) NCIMS-A prints master inventory listing	1	0.1	1	14	14	90.0	91	1274	18%	$27.53	$385	$2.75	$38.54	1000%
Totals	8.25	24.1		140	462		493	9674		$202.31	$6,644	$349.39	$31,398.89	
										10 Year Total	**$66,440**		**$313,989**	

**** Sub-processes that will be eliminated with UID/RFID implementation are 2, 3, 4 and 8.***

M) = 21%

M) = -79%

ROI is negative indicating an opportunity for IT enhancement.

Table 16. “To Be” Inventory Knowledge Value Analysis

Steps	Estimated Learning Time (ALT) (hrs.)	Work Time (hrs.)	Number of Employees	Number of times task completed (Annual)	Sum of task completion (Annual)	Knowledge Amount Embedded in IT (%)	Amount of Knowledge Units (per task)	Total Amount of Knowledge Units (Annual)	% Total Knowledge	Market Comparable Revenue	Total Market Comparable Revenue (Annual)	Process Cost		ROK
	A	B	C	D	E = A*C*D	F	G = (A*C)+F	H = E*G	I = G/TotalG	J	K = E*J	L = B*J		N = J/L
1) NCIMS-A prints inventory worksheets by location	1.75	0.25	1	52	91	90.0	91.75	8349.25	16%	$27.53	$2,505	$6.88		400%
2) Clerk conducts inventory of items with handheld device and data is transmitted wirelessly to NCIMS	0.625	2	2	52	65	95.0	96.25	6256.25	17%	$16.50	$1,073	$33.00		50%
3) NCIMS-A run exception report of missing items	1.75	0.15	1	52	91	90.0	91.75	8349.25	16%	$27.53	$2,505	$4.13		667%
4) Clerk conducts recount with handheld device and data is transmitted wirelessly to NCIMS	0.625	2.5	2	52	65	95.0	96.25	6256.25	17%	$8.25	$536	$20.63		40%
5) NCIMS-A prints final inventory discrepancy report	1.75	0.1	1	52	91	90.0	91.75	8349.25	16%	$27.53	$2,505	$2.75		1000%
6) NCIMS-A prints master inventory listing	1.75	0.1	1	52	91	90.0	91.75	8349.25	16%	$27.53	$2,505	$2.75		1000%
Totals	8.25	5.1		312	494		559.5	45909.5		$134.87	$11,630	$70.14		
										10 Year Total	**$116,297**			

al K / Total M) = **233%**
Total K) / Total M) = **133%**

ROK and ROI significantly improved by IT enhancement.

VIII. SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

A. SUMMARY

This project consisted of a review of both RFID and UID technologies that provided the reader a thorough background of what the individual technologies can and have brought to process improvement both within the DoD and the private sector. It covered technology, history, policy and on-going DoN initiatives of both RFID and UID. With that understanding, the project then analyzed an existing RFID/UID implementation at SPAWAR San Diego and identified how and why that system could be used at NSWC Crane.

The concurrent RFID/UID implementation plan for NSWC Crane was developed using the information from SPAWAR San Diego and the wireless security agreement from NSWC Carderock. The plan specifically addressed implementation at NSWC Crane's main warehouse facility and detailed a step-by step process to achieve operational approval. The plan provided who, what and when for completing the concurrent implementation; the why required further analysis.

To demonstrate the why of the implementation plan, the authors chose KVA analysis as a means to demonstrate a satisfactory return for this IT investment. That analysis proved that the concurrent implementation of RFID/UID significantly contributes to the inventory management process of NSWC Crane and meets the DoD's requirement as a worthwhile IT investment.

B. CONCLUSIONS

In 2006, the COMFISCS AIT Office established a group of Navy and commercial partners to take decisive action in implementing AIT across the Navy supply chain. As members of that group, we focused our efforts on the inventory management operations conducted at NSWC Crane. We analyzed the inventory workflow processes and assessed

the viability of concurrent RFID/UID implementation at that site. We conclude that this plan will bring to NSWC Crane the ability to meet DoD mandates with an efficient and effective solution for improving inventory management operations through RFID/UID implementation.

1. Meeting Department of Defense Mandates for RFID/UID Technology Implementation

The implementation of RFID and UID technology in military supply chain operations was mandated by the Department of Defense in 2003, but very few Navy organizations have complied with these directives so far. Adoption of the RFID/UID implementation plan discussed in this project will enable NSWC Crane to successfully fulfill the DoD's RFID and UID mandates. In addition to meeting those mandates, NSWC Crane will also realize numerous benefits of the concurrent implementation of RFID and UID technology.

2. Implementation of RFID/UID – An Efficient Solution

a. Concurrent Implementation – Two for the Price of One

Our observations and analysis determined that concurrent RFID/UID implementation is the right way forward. Concurrent implementation enables NSWC Crane to employ both technologies, saving time, labor and money, while meeting DoD mandates.

b. Knowledge Value Added by RFID/UID Implementation

RFID/UID Implementation dramatically increases the output of the inventory process while also improving the value (accuracy) of that output. The automation of certain sub-processes creates efficiency and reduces the amount of time to complete the sub-process.

c. *Realizing the Return On Knowledge (ROK) and Return On Investment (ROI)*

RFID/UID technology implementation increases both ROI and ROK ratios as the Market-Comparable Revenue of the inventory sub-process increases significantly compared to the Market-Comparable Process Cost. These ratios show a definite benefit to investing in RFID/UID technology and the value-added by AIT in inventory management.

d. *Improved Operations Efficiency and Improved Customer Services*

RFID/UID implementation translates to improved efficiency as both the amount and value of the output are enhanced. This leads to less time and resources wasted in rework and recounting. The time and resources available for other tasking and customer service is also increased.

e. *Improved Local Asset Visibility to Enterprise Wide Visibility*

Improved inventory accuracy drives success in achieving asset visibility. Asset visibility enables supply managers to plan and act in support of war fighters. RFID/UID implementation provides that inventory and asset visibility at the local level for NSWC Crane. This local level asset visibility is the foundation for the Navy and DoD in the quest for Total Asset Visibility (TAV). TAV will provide the leaders of the Navy and DoD with the capability to know and understand our true logistics readiness posture at all times and, in turn, drive improvements in operational readiness.

C. RECOMMENDATIONS

1. Expansion of NCIMS to NSWC Crane Small Arms Warehouse

The authors believe that future study should be devoted to the application of NCIMS at the NSWC Crane small arms warehouse with the existing inventory management system. Utilizing NCIMS at the small arms warehouse will provide desired levels of control and security while also increasing inventory accuracy. The methodology of KVA should be applied to this study to accurately capture the ROI.

2. NCIMS as a Model for Navy Supply Chain Application

The DoN should develop a policy to mandate a logistics network, similar to the NCIMS model, for all local Navy supply chain inventory/logistics IT systems. The policy developers should consult Ms. Jane Zimmerman of COMFISCS AIT for management and scheduling and Mr. Y.Y. Wong and Mr. Barry Jones of SPAWAR Code 4122 for technical aspects. The Navy's concurrent RFID/UID implementation will establish a standardized AIT system as a foundation of inventory and in-transit data collection to enhance TAV at a Navy-wide level.

3. DOD Mandate for RFID/UID Concurrent Implementation

The DoD should mandate an RFID/UID concurrent implementation policy that will provide automated TAV for inventory at rest and in-transit. The basic concept of concurrent AIT introduced by the logistics network, NCIMS, can be used as a model for DoD inventory control points and trans-shipment nodes. The corresponding data generated by such a network can be aggregated by USTRANSCOM to capture materiel movement and the information can then be distributed to logisticians and war fighters throughout the DoD.

LIST OF REFERENCES

107 Adams Communications. Bar code-1 2-Dimensional Bar Code Page. Retrieved on August 22, 2007, from http://www.adams1.com/pub/russadam/stack.html.

2D Matrix Barcodes White Paper. (2005). Retrieved on November 7, 2007, from http://www.visidot.com/files/2D_Data_Matrix-White_Paper.pdf.

Apte, U. M., Dew, N. & Ferrer, G. (2006). What is the Right RFID for Your Process? *Acquisition Research Sponsored Report Series,* 3-4, 9-27.

Command Information. (n.d.). Retrieved on September 27, 2007, from Space and Naval Warfare Systems Command:.http://enterprise.spawar.navy.mil.

Defense Procurement and Acquisition Policy. Retrieved on November 7, 2007 from http://www.acq.osd.mil/dpap/pdi/uid/index.html.

Department of Defense. (2007). *DoD Automatic Identification Technology Concept of Operations*, Version 2.0. Washington, D. C.: U.S. Government Printing Office.

Department of Defense. (2007). *United States Department of Defense Suppliers' Passive RFID Information Guide*, Version 9.0. Washington, D. C.: U.S. Government Printing Office.

Department of Defense, Office of the Under Secretary of Defense (Acquisition, Technology and Logistics). (July 29, 2003). Memorandum. Policy for Unique Identification (UID) of Tangible Items - New Equipment, Major Modifications, and Reprocurements of Equipment and Spares.

Department of the Navy. (2006). Navy Active RFID/In-Transit Visibility Concept of Operations (CONOPS).

Department of the Navy. (2005). United States Navy Radio Frequency Identification (RFID) Implementation Plan.

Estevez, A. F. & Geary, S. (2006). RFID: The Future is Now. *Exceptional Release.*

Estevez, Alan F. (2006). Army Logistician Bulletin. Retrieved on September 26, 2007, from http://www.almc.army.mil/ALOG/issues/MayJun05/pdf/alog_may_jun_05.pdf.

Extremely High Frequency (EHF) Satellite Communications (SATCOM). (2007). *Special Capabilities and Services.* Jones, B. Author.

Gaiser, R. L. Jr., & Hunt, C., From Acquisition to Distribution: Human Systems Integration in the Supply Chain.

Henley, B., personal communication, October 16, 2007.

Housel, T. and Bell, A. Measuring and Managing Knowledge. Boston: McGraw-Hill, 2001. pp. 92-93.

Housel, T.J. and Barretto, J. (2008). A Comparable Market Study of RFID for Manual Item-Level Accountability Inventory and Tracking Systems. In K.C. Laudon and J.P. Laudon, Management Information Systems (pp. H-1 – H-15). Upper Saddle River, New Jersey: Prentice Hall.

IUID toolkit. (2007). Retrieved on November 7, 2007, from http://www.iuidtookit.com.

Kann, J. (2004) Navy Supply Corps Newsletter. Understanding Unique Identification. Jan-Feb 2004.

Lahiri, S. (2005). *RFID Sourcebook*. Upper Saddle River, NJ: IBM Press. 1, 1-48.

Landit, J. (2001). Shrouds of time: *The History of RFID*, Retrieved on June 11, 2007, from http://www.transcore.com/pdf/AIM%20shrouds_of_time.pdf.

Naval Surface Warfare Center Carderock Division System Security Group. (2006). *System Security Authorization Agreement for Philadelphia Inventory Management System Wireless Complex.* Philadelphia, PA: U.S. Government Printing Office.

Navy AIT Technology Office. Automatic Identification Technology/Radio Frequency Identification. Retrieved on June 12, 2007, from, http://www.palm.saic.com/ait.htm.

Navy Passive RFID Business Case Analysis presentation. (May 8, 2007). Retrieved on November 10, 2007, from http://www.dla.mil/j-6/ait/Files/Conferences/Supply_Chain_Vis_Forum/Tuesday/T-5.%20%20Navy%20AIT%20Update.pdf.

Office of the Privacy Commissioner of Canada. Fact Sheet: RFID Technology. Retrieved on June 12, 2007, from http://www.privcom.gc.ca/fs-fi/02_05_d_28_e.asp.

Pavlou, P., Housel, T., Rodgers, W., & Jansen, E. July 2005. "Measuring the Return on Information Technology: A Knowledge-Based Approach for Revenue Allocation at the Process and Firm Level," Journal of the Association for Information Systems, Vol. 6, No.7, pp.199-226.

RFID use growing in automotive manufacturing process. (2007). *Industry Week.* Retrieved on July 13, 2007, from http://www.industryweek.com/ReadArticle.aspx?ArticleID=11774.

Rios, Cesar. Housel, Thomas. Mun, Jonathan. 2006. Integrated Portfolio Analysis: Return on Investment and Real Options Analysis of Intelligence Information Systems (Cryptologic Carry On Program). Naval Postgraduate School. pp. 2-13.

Sensing New RFID Opportunities. *RFID Journal*. Retrieved on July 13, 2007, from http://www.rfidjournal.com/article/articleview/2081/1/2/.

The Basics of RFID Technology. *RFID Journal* Retrieved on June 12, 2007, from http://www.rfidjournal.com/article/articleview/1337/1/129/.

The History of RFID Technology. *RFID Journal.* Retrieved on June 12, 2007, from http://www.rfidjournal.com/article/articleview/1338/1/129/.

Two Dimensional Bar Code Overview. (2006). Retrieved on September 26, 2007, from http://www.dataintro.com/lit/wp2dbarcodes.pdf.

What is automatic identification? *RFID Journal.* Retrieved on July 14, 2007, from http://www.rfidjournal.com/faq/16/49.

Who We Are, Command and Mission Statement. (n.d.). Retrieved on November 9, 2007, from Naval Surface Warfare Center Crane Division: http://www.crane.navy.mil/whoweare/.

Wong, Y. Y., and Jones, B. (2007, March). Using RFID and IUID to Reduce Life Cycle Costs Lessons Learned. Presentation.

Wong, Y. Y., and Jones, B. (2007, March). Introduction to Machine Readable Information. Presentation.

THIS PAGE LEFT INTENTIONALLY BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Geraldo Ferrer
   Naval Postgraduate School
   Monterey, California

4. Nick Dew
   Naval Postgraduate School
   Monterey, California

5. Jane Zimmerman
   COMFISCS
   San Diego, California

6. Capt. Michael Fulton
   NSWC Crane
   Crane, Indiana